

HPStorageWorks

Fabric OS 5.x diagnostics and system error messages reference guide

Legal and notice information

©Copyright 2005 Hewlett-Packard Development Company, L.P.

©Copyright 2005 Brocade Communications Systems, Incorporated.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information is provided "as is" without warranty of any kind and is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Intel and Itanium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Microsoft, Windows, Windows NT, and Windows XP are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Fabric OS 5.x diagnostics and system error messages reference guide

Contents

About this guide	77
Intended audience	77
Related documentation	77
Document conventions and symbols	78
HP technical support	79
HP-authorized reseller.	79
Helpful web sites	79
1 Introduction to System Messages	81
Message severity levels	81
Overview of the system messages	81
System message log (RASLog)	82
Audit logging	82
Dual-CP systems.	83
System logging daemon	83
Port logs	83
Panic dump and core dump files	83
Trace dumps	84
supportSave command	84
System console	84
View or configure the system message logs	84
Reading a system message	85
Example system message	85
Viewing system messages from AdvancedWeb Tools	87
Dumping the system messages.	87
Viewing the system messages with page breaks	88
Clearing the system message log	88
Responding to a system message	88
Looking up a system message	88
Gathering information	89
System module descriptions	89
2 Error messages	95
AUTH error messages	95
AUTH-1001	95
Message	95
Probable Cause	95
Recommended Action	95
Severity	95
Message	95
Probable Cause	95
Recommended Action	95
Severity	95
AUTH-1003	95
Message	95
Probable Cause	95
Recommended Action	95
Severity	96
AUTH-1004	96
Message	96
Probable Cause	96
Recommended Action	96
Severity	96
AUTH-1005	96

Message	96
Probable Cause	96
Recommended Action	96
Severity	96
AUTH-1006	96
Message	96
Probable Cause	96
Recommended Action	97
Severity	97
AUTH-1007	97
Message	97
Probable Cause	97
Recommended Action	97
Severity	97
AUTH-1008	97
Message	97
Probable Cause	97
Recommended Action	97
Severity	97
AUTH-1010	97
Message	97
Probable Cause	98
Recommended Action	98
Severity	98
AUTH-1011	98
Message	98
Probable Cause	98
Recommended Action	98
Severity	98
AUTH-1012	98
Message	98
Probable Cause	98
Recommended Action	98
Severity	98
AUTH-1013	99
Message	99
Probable Cause	99
Recommended Action	99
Severity	99
AUTH-1014	99
Message	99
Probable Cause	99
Recommended Action	99
Severity	99
AUTH-1017	99
Message	99
Probable Cause	99
Recommended Action	100
Severity	100
AUTH-1018	100
Message	100
Probable Cause	100
Recommended Action	100
Severity	100
AUTH-1020	100
Message	100
Probable Cause	100
Recommended Action	100
Severity	100

AUTH-1022	101
Message	101
Probable Cause	101
Recommended Action	101
Severity	101
AUTH-1023	101
Message	101
Probable Cause	101
Recommended Action	101
Severity	101
AUTH-1025	102
Message	102
Probable Cause	102
Recommended Action	102
Severity	102
AUTH-1027	102
Message	102
Probable Cause	102
Recommended Action	102
Severity	102
AUTH-1028	103
Message	103
Probable Cause	103
Recommended Action	103
Severity	103
AUTH-1029	103
Message	103
Probable Cause	103
Recommended Action	103
Severity	103
AUTH-1030	103
Message	103
Probable Cause	104
Recommended Action	104
Severity	104
AUTH-1031	104
Message	104
Probable Cause	104
Recommended Action	104
Severity	104
AUTH-1032	104
Message	104
Probable Cause	104
Recommended Action	104
Severity	105
AUTH-1033	105
Message	105
Probable Cause	105
Recommended Action	105
Severity	105
AUTH-1034	105
Message	105
Probable Cause	105
Recommended Action	105
Severity	105
AUTH-1035	105
Message	105
Probable Cause	105
Recommended Action	106

Severity	106
AUTH-1036	106
Message	106
Probable Cause	106
Recommended Action	106
Severity	106
AUTH-1037	106
Message	106
Probable Cause	106
Recommended Action	106
Severity	107
AUTH-1038	107
Message	107
Probable Cause	107
Recommended Action	107
Severity	107
BL error messages	107
BL-1000	107
Message	107
Probable Cause	107
Recommended Action	107
Severity	107
BL-1001	107
Message	107
Probable Cause	108
Recommended Action	108
Severity	108
BL-1002	108
Message	108
Probable Cause	108
Recommended Action	108
Severity	108
BL-1003	108
Message	108
Probable Cause	108
Recommended Action	108
Severity	109
BL-1004	109
Message	109
Probable Cause	109
Recommended Action	109
Severity	109
BL-1006	109
Message	109
Probable Cause	109
Recommended Action	109
Severity	109
BL-1007	109
Message	109
Probable Cause	110
Recommended Action	110
Severity	110
BL-1008	110
Message	110
Probable Cause	110
Recommended Action	110
Severity	110
BL-1009	110
Message	110

Probable Cause	110
Recommended Action	110
Severity	111
BL-1010	111
Message	111
Probable Cause	111
Recommended Action	111
Severity	111
BL-1011	111
Message	111
Probable Cause	111
Recommended Action	111
Severity	111
BL-1012	112
Message	112
Probable Cause	112
Recommended Action	112
Severity	112
BL-1013	112
Message	112
Probable Cause	112
Recommended Action	112
Severity	112
BL-1014	113
Message	113
Probable Cause	113
Recommended Action	113
Severity	113
BL-1015	113
Message	113
Probable Cause	113
Recommended Action	113
Severity	114
BL-1016	114
Message	114
Probable Cause	114
Recommended Action	114
Severity	114
BL-1017	114
Message	114
Probable Cause	114
Recommended Action	114
Severity	114
BL-1018	114
Message	114
Probable Cause	114
Recommended Action	115
Severity	115
BLL Error Messages	115
BLL-1000	115
Message	115
Probable Cause	115
Recommended Action	115
Severity	116
CDR error messages	116
CDR-1001	116
Message	116
Probable Cause	116
Recommended Action	116

Severity	116
CER-1001 error messages	116
CER-1001	116
Message	116
Probable Cause	116
Recommended Action	116
Severity	116
CONF error messages	117
CONF-1000	117
Message	117
Probable Cause	117
Recommended Action	117
Severity	117
EM error messages	117
EM-1001	117
Message	117
Probable Cause	117
Recommended Action	117
Severity	118
EM-1002	118
Message	118
Probable Cause	118
Recommended Action	118
Severity	118
EM-1003	118
Message	118
Probable Cause	118
Recommended Action	118
Severity	119
EM-1004	119
Message	119
Probable Cause	119
Recommended Action	119
Severity	119
EM-1005	119
Message	119
Probable Cause	120
Recommended Action	120
Severity	120
EM-1006	120
Message	120
Probable Cause	120
Recommended Action	120
Severity	120
EM-1007	120
Message	120
Probable Cause	120
Recommended Action	120
Severity	121
EM-1008	121
Message	121
Probable Cause	121
Recommended Action	121
Severity	121
EM-1009	121
Message	121
Probable Cause	121
Recommended Action	122
Severity	122

EM-1010	122
Message	122
Probable Cause	122
Recommended Action	122
Severity	122
EM-1011	122
Message	122
Probable Cause	122
Recommended Action	122
Severity	122
EM-1012	122
Message	122
Probable Cause	123
Recommended Action	123
Severity	123
EM-1013	123
Message	123
Probable Cause	123
Recommended Action	124
Severity	124
EM-1014	124
Message	124
Probable Cause	124
Recommended Action	124
Severity	124
EM-1015	124
Message	124
Probable Cause	125
Recommended Action	125
Severity	125
EM-1016	125
Message	125
Probable Cause	125
Recommended Action	125
Severity	125
EM-1017	125
Message	125
Probable Cause	125
Recommended Action	125
Severity	125
EM-1018	125
Message	125
Probable Cause	126
Recommended Action	126
Severity	126
EM-1019	126
Message	126
Probable Cause	126
Recommended Action	126
Severity	126
EM-1028	126
Message	126
Probable Cause	126
Recommended Action	127
Severity	127
EM-1029	127
Message	127
Probable Cause	127
Recommended Action	127

Severity	128
EM-1031	128
Message	128
Probable Cause	128
Recommended Action	128
Severity	128
EM-1033	128
Message	128
Probable Cause	128
Recommended Action	128
Severity	128
EM-1034	128
Message	128
Probable Cause	129
Recommended Action	129
Severity	129
EM-1035	129
Message	129
Probable Cause	129
Recommended Action	130
Severity	130
EM-1036	130
Message	130
Probable Cause	130
Recommended Action	130
Severity	130
EM-1041	130
Message	130
Probable Cause	130
Recommended Action	131
Severity	131
EM-1042	131
Message	131
Probable Cause	131
Recommended Action	132
Severity	132
EM-1043	132
Message	132
Probable Cause	132
Recommended Action	132
Severity	132
EM-1044	132
Message	132
Probable Cause	132
Recommended Action	132
Severity	132
EM-1045	132
Message	132
Probable Cause	132
Recommended Action	133
Severity	133
EM-1046	133
Message	133
Probable Cause	133
Recommended Action	133
Severity	133
EM-1047	133
Message	133
Probable Cause	133

Recommended Action	133
Severity	133
EM-1048	134
Message	134
Probable Cause	134
Recommended Action	134
Severity	134
EM-1049	134
Message	134
Probable Cause	134
Recommended Action	135
Severity	135
EM-1050	135
Message	135
Probable Cause	135
Recommended Action	135
Severity	136
EM-1051	136
Message	136
Probable Cause	136
Recommended Action	136
Severity	136
EM-1052	136
Message	136
Probable Cause	136
Recommended Action	137
Severity	137
EM-1053	137
Message	137
Probable Cause	137
Recommended Action	137
Severity	137
EM-1055	138
Message	138
Probable Cause	138
Recommended Action	138
Severity	138
EM-1056	138
Message	138
Probable Cause	138
Recommended Action	138
Severity	138
EM-1057	138
Message	138
Probable Cause	138
Recommended Action	138
Severity	139
EM-1058	139
Message	139
Probable Cause	139
Recommended Action	139
Severity	139
EM-1059	139
Message	139
Probable Cause	139
Recommended Action	139
Severity	139
EVMD error messages	139
EVMD-1001	139

Message	139
Probable Cause	139
Recommended Action	140
Severity	140
FABS error messages	140
FABR-1001	140
Message	140
Probable Cause	140
Recommended Action	140
Severity	140
FABR-1002	140
Message	140
Probable Cause	140
Recommended Action	140
Severity	140
FABR-1003	141
Message	141
Probable Cause	141
Recommended Action	141
Severity	141
FABR-1004	141
Message	141
Probable Cause	141
Recommended Action	141
Severity	141
FABR-1005	142
Message	142
Probable Cause	142
Recommended Action	142
Severity	142
FABR-1006	142
Message	142
Probable Cause	142
Recommended Action	142
Severity	142
FABR-1007	142
Message	142
Probable Cause	142
Recommended Action	143
Severity	143
FABR-1008	143
Message	143
Probable Cause	143
Recommended Action	143
Severity	143
FABR-1009	143
Message	143
Probable Cause	143
Recommended Action	143
Severity	143
FABR-1010	144
Message	144
Probable Cause	144
Recommended Action	144
Severity	144
FABR-1011	144
Message	144
Probable Cause	144
Recommended Action	144

Severity	144
FABR-1012	144
Message	144
Probable Cause	144
Recommended Action	144
Severity	145
FABR-1013	145
Message	145
Probable Cause	145
Recommended Action	145
Severity	145
FABR-1014	145
Message	145
Probable Cause	145
Recommended Action	145
Severity	145
FABR-1015	145
Message	145
Probable Cause	146
Recommended Action	146
Severity	146
FABR-1016	146
Message	146
Probable Cause	146
Recommended Action	146
Severity	146
FABR-1017	146
Message	146
Probable Cause	146
Recommended Action	146
Severity	146
FABR-1018	146
Message	146
Probable Cause	147
Recommended Action	147
Severity	147
FABR-1019	147
Message	147
Probable Cause	147
Recommended Action	147
Severity	147
FABR-1020	147
Message	147
Probable Cause	147
Recommended Action	148
Severity	148
FABR-1021	148
Message	148
Probable Cause	148
Recommended Action	148
Severity	148
FABR-1022	148
Message	148
Probable Cause	148
Recommended Action	148
Severity	148
FABR-1023	149
Message	149
Probable Cause	149

Recommended Action	149
Severity	149
FABR-1024	149
Message	149
Probable Cause	149
Recommended Action	149
Severity	149
FABR-1029	149
Message	149
Probable Cause	149
Recommended Action	150
Severity	150
FABR-1030	150
Message	150
Probable Cause	150
Recommended Action	150
Severity	150
FABS-1001	150
Message	150
Probable Cause	150
Recommended Action	150
Severity	150
FABS-1002	150
Message	150
Probable Cause	151
Recommended Action	151
Severity	151
FABS-1004	151
Message	151
Probable Cause	151
Recommended Action	151
Severity	151
FABS-1005	151
Message	151
Probable Cause	151
Recommended Action	151
Severity	151
FABS-1006	152
Message	152
Probable Cause	152
Recommended Action	152
Severity	152
FABS-1007	152
Message	152
Probable Cause	152
Recommended Action	152
Severity	152
FABS-1008	153
Message	153
Probable Cause	153
Recommended Action	153
Severity	153
FABS-1009	153
Message	153
Probable Cause	153
Recommended Action	153
Severity	153
FABS-1010	153
Message	153

Probable Cause	153
Recommended Action	153
Severity	153
FABS-1011	154
Message	154
Probable Cause	154
Recommended Action	154
Severity	154
FABS-1012	154
Message	154
Probable Cause	154
Recommended Action	154
Severity	154
FABS-1013	154
Message	154
Probable Cause	154
Recommended Action	154
Severity	155
FABS-1014	155
Message	155
Probable Cause	155
Recommended Action	155
Severity	155
FABS-1015	155
Message	155
Probable Cause	155
Recommended Action	155
Severity	155
FCMC error messages	156
FCMC-1001	156
Message	156
Probable Cause	156
Recommended Action	156
Severity	156
FCPD error messages	156
FCPD-1001	156
Message	156
Probable Cause	156
Recommended Action	156
Severity	156
FCPD-1002	156
Message	156
Probable Cause	157
Recommended Action	157
Severity	157
FCPD-1003	157
Message	157
Probable Cause	157
Recommended Action	157
Severity	157
FCPH error messages	157
FCPH-1001	157
Message	157
Probable Cause	157
Recommended Action	157
Severity	157
FICU error messages	158
FICU-1001	158
Message	158

Probable Cause	158
Recommended Action	158
Severity	158
FICU-1002.	158
Message	158
Probable Cause	158
Recommended Action	158
Severity	158
FICU-1003.	158
Message	158
Probable Cause	158
Recommended Action	159
Severity	159
FICU-1004.	159
Message	159
Probable Cause	159
Recommended Action	159
Severity	159
FICU-1005.	159
Message	159
Probable Cause	159
Recommended Action	159
Severity	159
FICU-1006.	160
Message	160
Probable Cause	160
Recommended Action	160
Severity	160
FICU-1007.	160
Message	160
Probable Cause	160
Recommended Action	160
Severity	160
FICU-1008.	160
Message	160
Probable Cause	160
Recommended Action	160
Severity	161
FICU-1009.	161
Message	161
Probable Cause	161
Recommended Action	161
Severity	161
FKLB error messages	161
FICU-1001.	161
Message	161
Probable Cause	161
Recommended Action	161
Severity	161
FICU-1002.	161
Message	161
Probable Cause	162
Recommended Action	162
Severity	162
FICU-1003.	162
Message	162
Probable Cause	162
Recommended Action	162
Severity	162

FICU-1004	162
Message	162
Probable Cause	162
Recommended Action	162
Severity	163
FICU-1005	163
Message	163
Probable Cause	163
Recommended Action	163
Severity	163
FICU-1006	163
Message	163
Probable Cause	163
Recommended Action	163
Severity	163
FICU-1007	163
Message	163
Probable Cause	163
Recommended Action	163
Severity	164
FICU-1008	164
Message	164
Probable Cause	164
Recommended Action	164
Severity	164
FICU-1009	164
Message	164
Probable Cause	164
Recommended Action	164
Severity	164
FICU-1010	164
Message	164
Probable Cause	164
Recommended Action	165
Severity	165
.	165
FLOD error messages	165
FLOD-1001	165
Message	165
Probable Cause	165
Recommended Action	165
Severity	165
FLOD-1003	165
Message	165
Probable Cause	165
Recommended Action	165
Severity	165
FLOD-1004	165
Message	165
Probable Cause	165
Recommended Action	166
Severity	166
FLOD-1005	166
Message	166
Probable Cause	166
Recommended Action	166
Severity	166
FLOD-1006	166
Message	166

Probable Cause	166
Recommended Action	166
Severity	166
FSPF error messages	166
FSPF-1001	166
Message	166
Probable Cause	166
Recommended Action	166
Severity	167
FSPF-1002	167
Message	167
Probable Cause	167
Recommended Action	167
Severity	167
FSPF-1003	167
Message	167
Probable Cause	167
Recommended Action	167
Severity	167
FSPF-1005	167
Message	167
Probable Cause	167
Recommended Action	168
Severity	168
FSPF-1006	168
Message	168
Probable Cause	168
Recommended Action	168
Severity	168
FSS error messages	168
FSS-1001	168
Message	168
Probable Cause	168
Recommended Action	168
Severity	168
FSS-1002	168
Message	168
Probable Cause	169
Recommended Action	169
Severity	169
FSS-1003	169
Message	169
Probable Cause	169
Recommended Action	169
Severity	169
FSS-1004	169
Message	169
Probable Cause	169
Recommended Action	169
Severity	169
FSS-1005	170
Message	170
Probable Cause	170
Recommended Action	170
Severity	170
FSS-1006	170
Message	170
Probable Cause	170
Recommended Action	170

Severity	170
FSSM errors	170
FSSM-1002	170
Message	170
Probable Cause	170
Recommended Action	170
Severity	170
FSSM-1003	171
Message	171
Probable Cause	171
Recommended Action	171
Severity	171
FSSM-1004	171
Message	171
Probable Cause	171
Recommended Action	171
Severity	171
FW error messages	171
FW-1001	171
Message	171
Probable Cause	172
Recommended Action	172
Severity	172
FW-1002	172
Message	172
Probable Cause	172
Recommended Action	172
Severity	172
FW-1003	172
Message	172
Probable Cause	172
Recommended Action	172
Severity	172
FW-1004	173
Message	173
Probable Cause	173
Recommended Action	173
Severity	173
FW-1005	173
Message	173
Probable Cause	173
Recommended Action	173
Severity	173
FW-1006	173
Message	173
Probable Cause	173
Recommended Action	173
Severity	174
FW-1007	174
Message	174
Probable Cause	174
Recommended Action	174
Severity	174
FW-1008	174
Message	174
Probable Cause	174
Recommended Action	174
Severity	174
FW-1009	174

Message	174
Probable Cause	174
Recommended Action	174
Severity	175
FW-1010	175
Message	175
Probable Cause	175
Recommended Action	175
Severity	175
FW-1011	175
Message	175
Probable Cause	175
Recommended Action	175
Severity	175
FW-1012	175
Message	175
Probable Cause	175
Recommended Action	176
Severity	176
FW-1033	176
Message	176
Probable Cause	176
Recommended Action	176
Severity	176
FW-1034	176
Message	176
Probable Cause	176
Recommended Action	176
Severity	176
FW-1035	176
Message	176
Probable Cause	176
Recommended Action	177
Severity	177
FW-1036	177
Message	177
Probable Cause	177
Recommended Action	177
Severity	177
FW-1037	177
Message	177
Probable Cause	177
Recommended Action	177
Severity	177
FW-1038	177
Message	177
Probable Cause	178
Recommended Action	178
Severity	178
FW-1039	178
Message	178
Probable Cause	178
Recommended Action	178
Severity	178
FW-1040	178
Message	178
Probable Cause	178
Recommended Action	178
Severity	178

FW-1041	179
Message	179
Probable Cause	179
Recommended Action	179
Severity	179
FW-1042	179
Message	179
Probable Cause	179
Recommended Action	179
Severity	179
FW-1043	179
Message	179
Probable Cause	179
Recommended Action	180
Severity	180
FW-1044	180
Message	180
Probable Cause	180
Recommended Action	180
Severity	180
FW-1045	180
Message	180
Probable Cause	180
Recommended Action	180
Severity	180
FW-1046	180
Message	180
Probable Cause	181
Recommended Action	181
Severity	181
FW-1047	181
Message	181
Probable Cause	181
Recommended Action	181
Severity	181
FW-1048	181
Message	181
Probable Cause	181
Recommended Action	181
Severity	181
FW-1049	181
Message	181
Probable Cause	182
Recommended Action	182
Severity	182
FW-1050	182
Message	182
Probable Cause	182
Recommended Action	182
Severity	182
FW-1051	182
Message	182
Probable Cause	182
Recommended Action	182
Severity	182
FW-1052	182
Message	182
Probable Cause	183
Recommended Action	183

Severity	183
FW-1113	183
Message	183
Probable Cause	183
Recommended Action	183
Severity	183
FW-1114	183
Message	183
Probable Cause	183
Recommended Action	183
Severity	183
FW-1115	184
Message	184
Probable Cause	184
Recommended Action	184
Severity	184
FW-1116	184
Message	184
Probable Cause	184
Recommended Action	184
Severity	184
FW-1117	184
Message	184
Probable Cause	184
Recommended Action	185
Severity	185
FW-1118	185
Message	185
Probable Cause	185
Recommended Action	185
Severity	185
FW-1119	185
Message	185
Probable Cause	185
Recommended Action	185
Severity	186
FW-1120	186
Message	186
Probable Cause	186
Recommended Action	186
Severity	186
FW-1121	186
Message	186
Probable Cause	186
Recommended Action	186
Severity	186
FW-1122	187
Message	187
Probable Cause	187
Recommended Action	187
Severity	187
FW-1123	187
Message	187
Probable Cause	187
Recommended Action	187
Severity	187
FW-1124	187
Message	187
Probable Cause	187

Recommended Action	188
Severity	188
FW-1125.	188
Message	188
Probable Cause	188
Recommended Action	188
Severity	188
FW-1126.	188
Message	188
Probable Cause	188
Recommended Action	188
Severity	188
FW-1127.	189
Message	189
Probable Cause	189
Recommended Action	189
Severity	189
FW-1128.	189
Message	189
Probable Cause	189
Recommended Action	189
Severity	189
FW-1129.	190
Message	190
Probable Cause	190
Recommended Action	190
Severity	190
FW-1130.	190
Message	190
Probable Cause	190
Recommended Action	190
Severity	190
FW-1131.	190
Message	190
Probable Cause	190
Recommended Action	190
Severity	191
FW-1132.	191
Message	191
Probable Cause	191
Recommended Action	191
Severity	191
FW-1133.	191
Message	191
Probable Cause	191
Recommended Action	191
Severity	191
FW-1134.	191
Message	191
Probable Cause	191
Recommended Action	192
Severity	192
FW-1135.	192
Message	192
Probable Cause	192
Recommended Action	192
Severity	192
FW-1136.	192
Message	192

Probable Cause	192
Recommended Action	192
Severity	192
FW-1137	192
Message	192
Probable Cause	193
Recommended Action	193
Severity	193
FW-1138	193
Message	193
Probable Cause	193
Recommended Action	193
Severity	193
FW-1139	193
Message	193
Probable Cause	193
Recommended Action	193
Severity	193
FW-1140	194
Message	194
Probable Cause	194
Recommended Action	194
Severity	194
FW-1160	194
Message	194
Probable Cause	194
Recommended Action	194
Severity	194
FW-1161	194
Message	194
Probable Cause	194
Recommended Action	195
Severity	195
FW-1162	195
Message	195
Probable Cause	195
Recommended Action	195
Severity	195
FW-1163	195
Message	195
Probable Cause	195
Recommended Action	195
Severity	195
FW-1164	196
Message	196
Probable Cause	196
Recommended Action	196
Severity	196
FW-1165	196
Message	196
Probable Cause	196
Recommended Action	196
Severity	196
FW-1166	196
Message	196
Probable Cause	196
Recommended Action	197
Severity	197
FW-1167	197

Message	197
Probable Cause	197
Recommended Action	197
Severity	197
FW-1168.	197
Message	197
Probable Cause	197
Recommended Action	197
Severity	197
FW-1169.	197
Message	197
Probable Cause	198
Recommended Action	198
Severity	198
FW-1170.	198
Message	198
Probable Cause	198
Recommended Action	198
Severity	198
FW-1171.	198
Message	198
Probable Cause	198
Recommended Action	198
Severity	198
FW-1172.	199
Message	199
Probable Cause	199
Recommended Action	199
Severity	199
FW-1173.	199
Message	199
Probable Cause	199
Recommended Action	199
Severity	199
FW-1174.	199
Message	199
Probable Cause	199
Recommended Action	199
Severity	200
FW-1175.	200
Message	200
Probable Cause	200
Recommended Action	200
Severity	200
FW-1176.	200
Message	200
Probable Cause	200
Recommended Action	200
Severity	200
FW-1177.	200
Message	200
Probable Cause	200
Recommended Action	201
Severity	201
FW-1178.	201
Message	201
Probable Cause	201
Recommended Action	201
Severity	201

FW-1179	201
Message	201
Probable Cause	201
Recommended Action	201
Severity	201
FW-1180	201
Message	201
Probable Cause	202
Recommended Action	202
Severity	202
FW-1181	202
Message	202
Probable Cause	202
Recommended Action	202
Severity	202
FW-1182	202
Message	202
Probable Cause	202
Recommended Action	202
Severity	202
FW-1183	202
Message	202
Probable Cause	203
Recommended Action	203
Severity	203
FW-1184	203
Message	203
Probable Cause	203
Recommended Action	203
Severity	203
FW-1185	203
Message	203
Probable Cause	203
Recommended Action	203
Severity	203
FW-1186	204
Message	204
Probable Cause	204
Recommended Action	204
Severity	204
FW-1187	204
Message	204
Probable Cause	204
Recommended Action	204
Severity	204
FW-1188	204
Message	204
Probable Cause	204
Recommended Action	204
Severity	205
FW-1189	205
Message	205
Probable Cause	205
Recommended Action	205
Severity	205
FW-1190	205
Message	205
Probable Cause	205
Recommended Action	205

Severity	205
FW-1191	205
Message	205
Probable Cause	205
Recommended Action	206
Severity	206
FW-1192	206
Message	206
Probable Cause	206
Recommended Action	206
Severity	206
FW-1193	206
Message	206
Probable Cause	206
Recommended Action	206
Severity	206
FW-1194	207
Message	207
Probable Cause	207
Recommended Action	207
Severity	207
FW-1195	207
Message	207
Probable Cause	207
Recommended Action	207
Severity	207
FW-1216	207
Message	207
Probable Cause	207
Recommended Action	208
Severity	208
FW-1217	208
Message	208
Probable Cause	208
Recommended Action	208
Severity	208
FW-1218	208
Message	208
Probable Cause	208
Recommended Action	208
Severity	209
FW-1219	209
Message	209
Probable Cause	209
Recommended Action	209
Severity	209
FW-1240	209
Message	209
Probable Cause	209
Recommended Action	209
Severity	209
FW-1241	209
Message	209
Probable Cause	210
Recommended Action	210
Severity	210
FW-1242	210
Message	210
Probable Cause	210

Recommended Action	210
Severity	210
FW-1243	210
Message	210
Probable Cause	210
Recommended Action	210
Severity	211
FW-1244	211
Message	211
Probable Cause	211
Recommended Action	211
Severity	211
FW-1245	211
Message	211
Probable Cause	211
Recommended Action	211
Severity	211
FW-1246	211
Message	211
Probable Cause	211
Recommended Action	212
Severity	212
FW-1247	212
Message	212
Probable Cause	212
Recommended Action	212
Severity	212
FW-1248	212
Message	212
Probable Cause	212
Recommended Action	212
Severity	212
FW-1249	212
Message	212
Probable Cause	213
Recommended Action	213
Severity	213
FW-1250	213
Message	213
Probable Cause	213
Recommended Action	213
Severity	213
FW-1251	213
Message	213
Probable Cause	213
Recommended Action	213
Severity	213
FW-1272	214
Message	214
Probable Cause	214
Recommended Action	214
Severity	214
FW-1273	214
Message	214
Probable Cause	214
Recommended Action	214
Severity	214
FW-1274	214
Message	214

Probable Cause	214
Recommended Action	215
Severity	215
FW-1275	215
Message	215
Probable Cause	215
Recommended Action	215
Severity	215
FW-1296	215
Message	215
Probable Cause	215
Recommended Action	215
Severity	215
FW-1297	216
Message	216
Probable Cause	216
Recommended Action	216
Severity	216
FW-1298	216
Message	216
Probable Cause	216
Recommended Action	216
Severity	216
FW-1299	216
Message	216
Probable Cause	216
Recommended Action	217
Severity	217
FW-1300	217
Message	217
Probable Cause	217
Recommended Action	217
Severity	217
FW-1301	217
Message	217
Probable Cause	217
Recommended Action	217
Severity	217
FW-1302	218
Message	218
Probable Cause	218
Recommended Action	218
Severity	218
FW-1303	218
Message	218
Probable Cause	218
Recommended Action	218
Severity	218
FW-1304	218
Message	218
Probable Cause	218
Recommended Action	219
Severity	219
FW-1305	219
Message	219
Probable Cause	219
Recommended Action	219
Severity	219
FW-1306	219

Message	219
Probable Cause	219
Recommended Action	219
Severity	219
FW-1307	220
Message	220
Probable Cause	220
Recommended Action	220
Severity	220
FW-1308	220
Message	220
Probable Cause	220
Recommended Action	220
Severity	220
FW-1309	220
Message	220
Probable Cause	220
Recommended Action	221
Severity	221
FW-1310	221
Message	221
Probable Cause	221
Recommended Action	221
Severity	221
FW-1311	221
Message	221
Probable Cause	221
Recommended Action	221
Severity	221
FW-1312	221
Message	221
Probable Cause	222
Recommended Action	222
Severity	222
FW-1313	222
Message	222
Probable Cause	222
Recommended Action	222
Severity	222
FW-1314	222
Message	222
Probable Cause	222
Recommended Action	222
Severity	222
FW-1315	223
Message	223
Probable Cause	223
Recommended Action	223
Severity	223
FW-1316	223
Message	223
Probable Cause	223
Recommended Action	223
Severity	223
FW-1317	223
Message	223
Probable Cause	223
Recommended Action	224
Severity	224

FW-1318	224
Message	224
Probable Cause	224
Recommended Action	224
Severity	224
FW-1319	224
Message	224
Probable Cause	224
Recommended Action	224
Severity	224
FW-1320	225
Message	225
Probable Cause	225
Recommended Action	225
Severity	225
FW-1321	225
Message	225
Probable Cause	225
Recommended Action	225
Severity	225
FW-1322	225
Message	225
Probable Cause	225
Recommended Action	226
Severity	226
FW-1323	226
Message	226
Probable Cause	226
Recommended Action	226
Severity	226
FW-1324	226
Message	226
Probable Cause	226
Recommended Action	226
Severity	226
FW-1325	227
Message	227
Probable Cause	227
Recommended Action	227
Severity	227
FW-1326	227
Message	227
Probable Cause	227
Recommended Action	227
Severity	227
FW-1327	227
Message	227
Probable Cause	227
Recommended Action	228
Severity	228
FW-1328	228
Message	228
Probable Cause	228
Recommended Action	228
Severity	228
FW-1329	228
Message	228
Probable Cause	228
Recommended Action	228

Severity	228
FW-1330	228
Message	228
Probable Cause	229
Recommended Action	229
Severity	229
FW-1331	229
Message	229
Probable Cause	229
Recommended Action	229
Severity	229
FW-1332	229
Message	229
Probable Cause	229
Recommended Action	229
Severity	229
FW-1333	230
Message	230
Probable Cause	230
Recommended Action	230
Severity	230
FW-1334	230
Message	230
Probable Cause	230
Recommended Action	230
Severity	230
FW-1335	230
Message	230
Probable Cause	230
Recommended Action	231
Severity	231
FW-1336	231
Message	231
Probable Cause	231
Recommended Action	231
Severity	231
FW-1337	231
Message	231
Probable Cause	231
Recommended Action	231
Severity	231
FW-1338	232
Message	232
Probable Cause	232
Recommended Action	232
Severity	232
FW-1339	232
Message	232
Probable Cause	232
Recommended Action	232
Severity	232
FW-1340	232
Message	232
Probable Cause	233
Recommended Action	233
Severity	233
FW-1341	233
Message	233
Probable Cause	233

Recommended Action	233
Severity	233
FW-1342.	233
Message	233
Probable Cause	233
Recommended Action	233
Severity	233
FW-1343.	234
Message	234
Probable Cause	234
Recommended Action	234
Severity	234
FW-1344.	234
Message	234
Probable Cause	234
Recommended Action	234
Severity	234
FW-1345.	234
Message	234
Probable Cause	234
Recommended Action	235
Severity	235
FW-1346.	235
Message	235
Probable Cause	235
Recommended Action	235
Severity	235
FW-1347.	235
Message	235
Probable Cause	235
Recommended Action	235
Severity	235
FW-1348.	236
Message	236
Probable Cause	236
Recommended Action	236
Severity	236
FW-1349.	236
Message	236
Probable Cause	236
Recommended Action	236
Severity	236
FW-1350.	236
Message	236
Probable Cause	237
Recommended Action	237
Severity	237
FW-1351.	237
Message	237
Probable Cause	237
Recommended Action	237
Severity	237
FW-1352.	237
Message	237
Probable Cause	237
Recommended Action	238
Severity	238
FW-1353.	238
Message	238

Probable Cause	238
Recommended Action	238
Severity	238
FW-1354	238
Message	238
Probable Cause	238
Recommended Action	238
Severity	238
FW-1355	239
Message	239
Probable Cause	239
Recommended Action	239
Severity	239
FW-1356	239
Message	239
Probable Cause	239
Recommended Action	239
Severity	239
FW-1357	239
Message	239
Probable Cause	240
Recommended Action	240
Severity	240
FW-1358	240
Message	240
Probable Cause	240
Recommended Action	240
Severity	240
FW-1359	240
Message	240
Probable Cause	240
Recommended Action	240
Severity	240
FW-1360	241
Message	241
Probable Cause	241
Recommended Action	241
Severity	241
FW-1361	241
Message	241
Probable Cause	241
Recommended Action	241
Severity	241
FW-1362	241
Message	241
Probable Cause	241
Recommended Action	241
Severity	242
FW-1363	242
Message	242
Probable Cause	242
Recommended Action	242
Severity	242
FW-1364	242
Message	242
Probable Cause	242
Recommended Action	242
Severity	242
FW-1365	242

Message	242
Probable Cause	242
Recommended Action	242
Severity	243
FW-1366	243
Message	243
Probable Cause	243
Recommended Action	243
Severity	243
FW-1367	243
Message	243
Probable Cause	243
Recommended Action	243
Severity	243
FW-1368	243
Message	243
Probable Cause	243
Recommended Action	244
Severity	244
FW-1369	244
Message	244
Probable Cause	244
Recommended Action	244
Severity	244
FW-1370	244
Message	244
Probable Cause	244
Recommended Action	244
Severity	244
FW-1371	245
Message	245
Probable Cause	245
Recommended Action	245
Severity	245
FW-1372	245
Message	245
Probable Cause	245
Recommended Action	245
Severity	245
FW-1373	245
Message	245
Probable Cause	245
Recommended Action	246
Severity	246
FW-1374	246
Message	246
Probable Cause	246
Recommended Action	246
Severity	246
FW-1375	246
Message	246
Probable Cause	246
Recommended Action	246
Severity	246
FW-1376	247
Message	247
Probable Cause	247
Recommended Action	247
Severity	247

FW-1377	247
Message	247
Probable Cause	247
Recommended Action	247
Severity	247
FW-1378	247
Message	247
Probable Cause	247
Recommended Action	248
Severity	248
FW-1379	248
Message	248
Probable Cause	248
Recommended Action	248
Severity	248
FW-1400	248
Message	248
Probable Cause	248
Recommended Action	248
Severity	248
FW-1401	249
Message	249
Probable Cause	249
Recommended Action	249
Severity	249
FW-1402	249
Message	249
Probable Cause	249
Recommended Action	249
Severity	249
FW-1403	249
Message	249
Probable Cause	249
Recommended Action	250
Severity	250
FW-1424	250
Message	250
Probable Cause	250
Recommended Action	250
Severity	250
FW-1425	250
Message	250
Probable Cause	250
Recommended Action	250
Severity	250
FW-1426	250
Message	250
Probable Cause	250
Recommended Action	251
Severity	251
FW-1427	251
Message	251
Probable Cause	251
Recommended Action	251
Severity	251
FW-1428	251
Message	251
Probable Cause	251
Recommended Action	251

Severity	251
FW-1429	251
Message	251
Probable Cause	251
Recommended Action	252
Severity	252
FW-1430	252
Message	252
Probable Cause	252
Recommended Action	252
Severity	252
FW-1431	252
Message	252
Probable Cause	252
Recommended Action	252
Severity	252
FW-1432	252
Message	252
Probable Cause	252
Recommended Action	253
Severity	253
FW-1433	253
Message	253
Probable Cause	253
Recommended Action	253
Severity	253
FW-1434	253
Message	253
Probable Cause	253
Recommended Action	253
Severity	253
FW-1435	254
Message	254
Probable Cause	254
Recommended Action	254
Severity	254
FW-1436	254
Message	254
Probable Cause	254
Recommended Action	254
Severity	254
FW-1437	254
Message	254
Probable Cause	254
Recommended Action	254
Severity	255
FW-1438	255
Message	255
Probable Cause	255
Recommended Action	255
Severity	255
FW-1439	255
Message	255
Probable Cause	255
Recommended Action	255
Severity	255
FW-1440	255
Message	255
Probable Cause	255

	Recommended Action	255
	Severity	255
	FW-1441	256
	Message	256
	Probable Cause	256
	Recommended Action	256
	Severity	256
	FW-1442	256
	Message	256
	Probable Cause	256
	Recommended Action	256
	Severity	256
	FW-1443	256
	Message	256
	Probable Cause	256
	Recommended Action	256
	Severity	256
	FW-1444	257
	Message	257
	Probable Cause	257
	Recommended Action	257
	Severity	257
HAM	error messages	257
	HAM-1001	257
	Message	257
	Probable Cause	257
	Recommended Action	257
	Severity	257
	HAM-1002	257
	Message	257
	Probable Cause	257
	Recommended Action	257
	Severity	258
	HAM-1004	258
	Message	258
	Probable Cause	258
	Recommended Action	258
	Severity	258
HAMK	error messages	258
	HAMK-1002	258
	Message	258
	Probable Cause	259
	Recommended Action	259
	Severity	259
	HAMK-1003	259
	Message	259
	Probable Cause	259
	Recommended Action	259
	Severity	259
	HAMK-1004	259
	Message	259
	Probable Cause	259
	Recommended Action	259
	Severity	259
HIL	Error Messages	260
	HIL-1101	260
	Message	260
	Probable Cause	260
	Recommended Action	260

Severity	260
HIL-1102	260
Message	260
Probable Cause	260
Recommended Action	260
Severity	260
HIL-1103	260
Message	260
Probable Cause	260
Recommended Action	260
Severity	261
HIL-1104	261
Message	261
Probable Cause	261
Recommended Action	261
Severity	261
HIL-1105	261
Message	261
Probable Cause	261
Recommended Action	261
Severity	261
HIL-1106	261
Message	261
Probable Cause	262
Recommended Action	262
Severity	262
HIL-1107	262
Message	262
Probable Cause	262
Recommended Action	262
Severity	262
HIL-1108	262
Message	262
Probable Cause	262
Recommended Action	262
Severity	263
HIL-1201	263
Message	263
Probable Cause	263
Recommended Action	263
Severity	263
HIL-1202	263
Message	263
Probable Cause	263
Recommended Action	263
Severity	264
HIL-1203	264
Message	264
Probable Cause	264
Recommended Action	264
Severity	264
HIL-1204	264
Message	264
Probable Cause	264
Recommended Action	264
Severity	265
HIL-1205	265
Message	265
Probable Cause	265

Recommended Action	265
Severity	265
HIL-1206	265
Message	265
Probable Cause	265
Recommended Action	265
Severity	266
HIL-1207	266
Message	266
Probable Cause	266
Recommended Action	266
Severity	266
HIL-1301	266
Message	266
Probable Cause	266
Recommended Action	266
Severity	266
HIL-1302	267
Message	267
Probable Cause	267
Recommended Action	267
Severity	267
HIL-1303	267
Message	267
Probable Cause	267
Recommended Action	267
Severity	267
HIL-1304	268
Message	268
Probable Cause	268
Recommended Action	268
Severity	268
HIL-1305	268
Message	268
Probable Cause	268
Recommended Action	268
Severity	268
HIL-1306	268
Message	268
Probable Cause	269
Recommended Action	269
Severity	269
HIL-1307	269
Message	269
Probable Cause	269
Recommended Action	269
Severity	269
HIL-1308	269
Message	269
Probable Cause	269
Recommended Action	269
Severity	270
HIL-1309	270
Message	270
Probable Cause	270
Recommended Action	270
Severity	270
HIL-1310	270
Message	270

Probable Cause	270
Recommended Action	270
Severity	270
HIL-1401	271
Message	271
Probable Cause	271
Recommended Action	271
Severity	271
HIL-1402	271
Message	271
Probable Cause	271
Recommended Action	271
Severity	271
HIL-1403	271
Message	271
Probable Cause	271
Recommended Action	271
Severity	271
HIL-1404	272
Message	272
Probable Cause	272
Recommended Action	272
Severity	272
HIL-1501	272
Message	272
Probable Cause	272
Recommended Action	272
Severity	272
HIL-1502	272
Message	272
Probable Cause	272
Recommended Action	273
Severity	273
HIL-1503	273
Message	273
Probable Cause	273
Recommended Action	273
Severity	273
HIL-1504	273
Message	273
Probable Cause	273
Recommended Action	273
Severity	274
HIL-1505	274
Message	274
Probable Cause	274
Recommended Action	274
Severity	274
HIL-1506	274
Message	274
Probable Cause	274
Recommended Action	274
Severity	274
HIL-1507	275
Message	275
Probable Cause	275
Recommended Action	275
Severity	275
HIL-1508	275

Message	275
Probable Cause	275
Recommended Action	275
Severity	275
HIL-1509	276
Message	276
Probable Cause	276
Recommended Action	276
Severity	276
HIL-1601	276
Message	276
Probable Cause	276
Recommended Action	276
Severity	276
HIL-1602	276
Message	276
Probable Cause	276
Recommended Action	277
Severity	277
HLO error messages	277
HLO-1001	277
Message	277
Probable Cause	277
Recommended Action	277
Severity	277
HLO-1002	277
Message	277
Probable Cause	277
Recommended Action	277
Severity	277
HLO-1003	278
Message	278
Probable Cause	278
Recommended Action	278
Severity	278
HMON error messages	278
HMON-1001	278
Message	278
Probable Cause	278
Recommended Action	278
Severity	278
HTTP error messages	278
HTTP-1001	278
Message	278
Probable Cause	279
Recommended Action	279
Severity	279
KSWD error messages	279
KSWD-1003	279
Message	279
Probable Cause	279
Recommended Action	279
Severity	279
KTRC error messages	279
KTRC-1001	279
Message	279
Probable Cause	279
Recommended Action	280
Severity	280

KTRC-1002	280
Message	280
Probable Cause	280
Recommended Action	280
Severity	280
KTRC-1003	280
Message	280
Probable Cause	280
Recommended Action	280
Severity	280
KTRC-1004	280
Message	280
Probable Cause	280
Recommended Action	280
Severity	280
LOG Error Messages	281
LOG-1000	281
Message	281
Probable Cause	281
Recommended Action	281
Severity	281
LOG-1001	281
Message	281
Probable Cause	281
Recommended Action	281
Severity	281
LOG-1002	281
Message	281
Probable Cause	281
Recommended Action	281
Severity	282
LSDB Error Messages	282
LSDB-1001	282
Message	282
Probable Cause	282
Recommended Action	282
Severity	282
LSDB-1002	282
Message	282
Probable Cause	282
Recommended Action	282
Severity	282
LSDB-1003	282
Message	282
Probable Cause	283
Recommended Action	283
Severity	283
LSDB-1004	283
Message	283
Probable Cause	283
Recommended Action	283
Severity	283
MFIC Error Messages	283
MFIC-1001	283
Message	283
Probable Cause	283
Recommended Action	283
Severity	283
MFIC-1002	284

Message	284
Probable Cause	284
Recommended Action	284
Severity	284
MFIC-1003	284
Message	284
Probable Cause	284
Recommended Action	284
Severity	284
MPTH Error Messages	284
MPTH-1001	284
Message	284
Probable Cause	285
Recommended Action	285
Severity	285
MPTH-1002	285
Message	285
Probable Cause	285
Recommended Action	285
Severity	285
MPTH-1003	285
Message	285
Probable Cause	285
Recommended Action	285
Severity	285
MQ Error Messages	285
MQ-1004	285
Message	285
Probable Cause	286
Recommended Action	286
Severity	286
MS Error Messages	286
MS-1001	286
Message	286
Probable Cause	286
Recommended Action	286
Severity	286
MS-1002	286
Message	286
Probable Cause	287
Recommended Action	287
Severity	287
MS-1003	287
Message	287
Probable Cause	287
Recommended Action	287
Severity	288
MS-1004	288
Message	288
Probable Cause	288
Recommended Action	288
Severity	288
MS-1005	288
Message	288
Probable Cause	288
Recommended Action	288
Severity	288
MS-1006	289
Message	289

Probable Cause	289
Recommended Action	289
Severity	289
MS-1008	289
Message	289
Probable Cause	289
Recommended Action	289
Severity	289
MS-1021	289
Message	289
Probable Cause	289
Recommended Action	290
Severity	290
NBFS Error Messages	290
NBFS-1001	290
Message	290
Probable Cause	290
Recommended Action	290
Severity	290
NBFS-1002	290
Message	290
Probable Cause	290
Recommended Action	291
Severity	291
NBFS-1003	291
Message	291
Probable Cause	291
Recommended Action	291
Severity	291
NS Error Messages	291
NS-1001	291
Message	291
Probable Cause	291
Recommended Action	291
Severity	292
NS-1002	292
Message	292
Probable Cause	292
Recommended Action	292
Severity	292
NS-1003	292
Message	292
Probable Cause	292
Recommended Action	292
Severity	292
NS-1004	292
Message	292
Probable Cause	293
Recommended Action	293
Severity	293
PDM Error Messages	293
PDM-1001	293
Message	293
Probable Cause	293
Recommended Action	293
Severity	293
PDM-1002	293
Message	293
Probable Cause	293

Recommended Action	293
Severity	293
PDM-1003.	294
Message	294
Probable Cause	294
Recommended Action	294
Severity	294
PDM-1004.	294
Message	294
Probable Cause	294
Recommended Action	294
Severity	294
PDM-1005.	294
Message	294
Probable Cause	294
Recommended Action	294
Severity	295
PDM-1006.	295
Message	295
Probable Cause	295
Recommended Action	295
Severity	295
PDM-1007.	295
Message	295
Probable Cause	295
Recommended Action	295
Severity	295
PDM-1008.	295
Message	295
Probable Cause	295
Recommended Action	295
Severity	296
PDM-1009.	296
Message	296
Probable Cause	296
Recommended Action	296
Severity	296
PDM-1010.	296
Message	296
Probable Cause	296
Recommended Action	296
Severity	296
PDM-1011.	296
Message	296
Probable Cause	296
Recommended Action	297
Severity	297
PDM-1012.	297
Message	297
Probable Cause	297
Recommended Action	297
Severity	297
PDM-1013.	297
Message	297
Probable Cause	297
Recommended Action	297
Severity	297
PDM-1014.	297
Message	297

Probable Cause	298
Recommended Action	298
Severity	298
PDM-1017	298
Message	298
Probable Cause	298
Recommended Action	298
Severity	298
PDM-1019	298
Message	298
Probable Cause	298
Recommended Action	298
Severity	298
PDM-1020	299
Message	299
Probable Cause	299
Recommended Action	299
Severity	299
PDM-1021	299
Message	299
Probable Cause	299
Recommended Action	299
Severity	299
PDTR Error Messages	299
PDTR-1001	299
Message	299
Probable Cause	299
Recommended Action	299
Severity	300
PDTR-1002	300
Message	300
Probable Cause	300
Recommended Action	300
Severity	300
PLAT Error Messages	300
PLAT-1000	300
Message	300
Probable Cause	300
Recommended Action	300
Severity	300
PLAT-1001	300
Message	300
Probable Cause	301
Recommended Action	301
Severity	301
.	301
PORT Error Messages	301
PORT-1003	301
Message	301
Probable Cause	301
Recommended Action	301
Severity	301
PORT-1004	301
Message	301
Probable Cause	301
Recommended Action	301
Severity	302
PS Error Messages	302
PS-1000	302

Message	302
Probable Cause	302
Recommended Action	302
Severity	302
PS-1001	302
Message	302
Probable Cause	302
Recommended Action	302
Severity	302
PS-1002	302
Message	302
Probable Cause	302
Recommended Action	303
Severity	303
PS-1003	303
Message	303
Probable Cause	303
Recommended Action	303
Severity	303
PS-1004	303
Message	303
Probable Cause	303
Recommended Action	303
Severity	303
PS-1005	303
Message	303
Probable Cause	303
Recommended Action	304
Severity	304
PSWP Error Messages	304
PSWP-1001	304
Message	304
Probable Cause	304
Recommended Action	304
Severity	304
PSWP-1002	304
Message	304
Probable Cause	304
Recommended Action	304
Severity	304
PSWP-1003	304
Message	304
Probable Cause	304
Recommended Action	305
Severity	305
PSWP-1004	305
Message	305
Probable Cause	305
Recommended Action	305
Severity	305
RCS Error Messages	305
RCS-1001	305
Message	305
Probable Cause	305
Recommended Action	305
Severity	305
RCS-1002	305
Message	305
Probable Cause	306

Recommended Action	306
Severity	306
RCS-1003	306
Message	306
Probable Cause	306
Recommended Action	306
Severity	306
RCS-1004	306
Message	306
Probable Cause	306
Recommended Action	306
Severity	306
RCS-1005	307
Message	307
Probable Cause	307
Recommended Action	307
Severity	307
RCS-1006	307
Message	307
Probable Cause	307
Recommended Action	307
Severity	307
RCS-1007	307
Message	307
Probable Cause	308
Recommended Action	308
Severity	308
RCS-1008	308
Message	308
Probable Cause	308
Recommended Action	308
Severity	308
RPCD Error Messages.	308
RPCD-1001	308
Message	308
Probable Cause	308
Recommended Action	308
Severity	308
RPCD-1002	308
Message	308
Probable Cause	308
Recommended Action	309
Severity	309
RPCD-1003	309
Message	309
Probable Cause	309
Recommended Action	309
Severity	309
RPCD-1004	309
Message	309
Probable Cause	309
Recommended Action	309
Severity	309
RPCD-1005	309
Message	309
Probable Cause	309
Recommended Action	309
Severity	310
RPCD-1006	310

Message	310
Probable Cause	310
Recommended Action	310
Severity	310
RPCD-1007	310
Message	310
Probable Cause	310
Recommended Action	310
Severity	310
RTWR Error Messages	310
RTWR-1001	310
Message	310
Probable Cause	310
Recommended Action	310
Severity	311
RTWR-1002	311
Message	311
Probable Cause	311
Recommended Action	311
Severity	311
RTWR-1003	311
Message	311
Probable Cause	311
Recommended Action	311
Severity	311
SCN Error Messages	312
SCN-1001	312
Message	312
Probable Cause	312
Recommended Action	312
Severity	312
SEC Error Messages	312
SEC-1001	312
Message	312
Probable Cause	312
Recommended Action	313
Severity	313
SEC-1002	313
Message	313
Probable Cause	313
Recommended Action	313
Severity	313
SEC-1003	313
Message	313
Probable Cause	313
Recommended Action	313
Severity	314
SEC-1005	314
Message	314
Probable Cause	314
Recommended Action	314
Severity	314
SEC-1006	314
Message	314
Probable Cause	314
Recommended Action	314
Severity	314
SEC-1007	314
Message	314

Probable Cause	315
Recommended Action	315
Severity	315
SEC-1008	315
Message	315
Probable Cause	315
Recommended Action	315
Severity	315
SEC-1009	315
Message	315
Probable Cause	315
Recommended Action	315
Severity	315
SEC-1016	315
Message	315
Probable Cause	316
Recommended Action	316
Severity	316
SEC-1022	316
Message	316
Probable Cause	316
Recommended Action	316
Severity	316
SEC-1024	316
Message	316
Probable Cause	316
Recommended Action	316
Severity	316
SEC-1025	316
Message	316
Probable Cause	317
Recommended Action	317
Severity	317
SEC-1026	317
Message	317
Probable Cause	317
Recommended Action	317
Severity	317
SEC-1028	317
Message	317
Probable Cause	317
Recommended Action	317
Severity	317
SEC-1029	318
Message	318
Probable Cause	318
Recommended Action	318
Severity	318
SEC-1030	318
Message	318
Probable Cause	318
Recommended Action	318
Severity	318
SEC-1031	318
Message	318
Probable Cause	318
Recommended Action	318
Severity	319
SEC-1032	319

Message	319
Probable Cause	319
Recommended Action	319
Severity	319
SEC-1033	319
Message	319
Probable Cause	319
Recommended Action	319
Severity	319
SEC-1034	319
Message	319
Probable Cause	319
Recommended Action	320
Severity	320
SEC-1035	320
Message	320
Probable Cause	320
Recommended Action	320
Severity	320
SEC-1036	320
Message	320
Probable Cause	320
Recommended Action	320
Severity	320
SEC-1037	320
Message	320
Probable Cause	320
Recommended Action	321
Severity	321
SEC-1038	321
Message	321
Probable Cause	321
Recommended Action	321
Severity	321
SEC-1040	321
Message	321
Probable Cause	321
Recommended Action	321
Severity	321
SEC-1041	321
Message	321
Probable Cause	322
Recommended Action	322
Severity	322
SEC-1042	322
Message	322
Probable Cause	322
Recommended Action	322
Severity	322
SEC-1043	322
Message	322
Probable Cause	322
Recommended Action	322
Severity	322
SEC-1044	322
Message	322
Probable Cause	323
Recommended Action	323
Severity	323

SEC-1045	323
Message	323
Probable Cause	323
Recommended Action	323
Severity	323
SEC-1046	323
Message	323
Probable Cause	323
Recommended Action	323
Severity	323
SEC-1049	324
Message	324
Probable Cause	324
Recommended Action	324
Severity	324
SEC-1050	324
Message	324
Probable Cause	324
Recommended Action	324
Severity	324
SEC-1051	324
Message	324
Probable Cause	324
Recommended Action	325
Severity	325
SEC-1052	325
Message	325
Probable Cause	325
Recommended Action	325
Severity	325
SEC-1053	325
Message	325
Probable Cause	325
Recommended Action	325
Severity	325
SEC-1054	325
Message	325
Probable Cause	326
Recommended Action	326
Severity	326
SEC-1055	326
Message	326
Probable Cause	326
Recommended Action	326
Severity	326
SEC-1056	326
Message	326
Probable Cause	326
Recommended Action	326
Severity	326
SEC-1057	327
Message	327
Probable Cause	327
Recommended Action	327
Severity	327
SEC-1059	327
Message	327
Probable Cause	327
Recommended Action	327

Severity	327
SEC-1062	327
Message	327
Probable Cause	327
Recommended Action	327
Severity	327
SEC-1063	328
Message	328
Probable Cause	328
Recommended Action	328
Severity	328
SEC-1064	328
Message	328
Probable Cause	328
Recommended Action	328
Severity	328
SEC-1065	328
Message	328
Probable Cause	328
Recommended Action	328
Severity	328
SEC-1069	329
Message	329
Probable Cause	329
Recommended Action	329
Severity	329
SEC-1071	329
Message	329
Probable Cause	329
Recommended Action	329
Severity	329
SEC-1072	329
Message	329
Probable Cause	329
Recommended Action	329
Severity	329
SEC-1073	330
Message	330
Probable Cause	330
Recommended Action	330
Severity	330
SEC-1074	330
Message	330
Probable Cause	330
Recommended Action	330
Severity	330
SEC-1075	330
Message	330
Probable Cause	330
Recommended Action	330
Severity	331
SEC-1076	331
Message	331
Probable Cause	331
Recommended Action	331
Severity	331
SEC-1077	331
Message	331
Probable Cause	331

Recommended Action	331
Severity	331
SEC-1078	331
Message	331
Probable Cause	331
Recommended Action	331
Severity	332
SEC-1079	332
Message	332
Probable Cause	332
Recommended Action	332
Severity	332
SEC-1080	332
Message	332
Probable Cause	332
Recommended Action	332
Severity	332
SEC-1081	332
Message	332
Probable Cause	332
Recommended Action	333
Severity	333
SEC-1082	333
Message	333
Probable Cause	333
Recommended Action	333
Severity	333
SEC-1083	333
Message	333
Probable Cause	333
Recommended Action	333
Severity	333
SEC-1084	333
Message	333
Probable Cause	333
Recommended Action	334
Severity	334
SEC-1085	334
Message	334
Probable Cause	334
Recommended Action	334
Severity	334
SEC-1086	334
Message	334
Probable Cause	334
Recommended Action	334
Severity	334
SEC-1088	334
Message	334
Probable Cause	334
Recommended Action	335
Severity	335
SEC-1089	335
Message	335
Probable Cause	335
Recommended Action	335
Severity	335
SEC-1090	335
Message	335

Probable Cause	335
Recommended Action	335
Severity	335
SEC-1091	336
Message	336
Probable Cause	336
Recommended Action	336
Severity	336
SEC-1092	336
Message	336
Probable Cause	336
Recommended Action	336
Severity	336
SEC-1093	336
Message	336
Probable Cause	336
Recommended Action	336
Severity	337
SEC-1094	337
Message	337
Probable Cause	337
Recommended Action	337
Severity	337
SEC-1095	337
Message	337
Probable Cause	337
Recommended Action	337
Severity	337
SEC-1096	337
Message	337
Probable Cause	337
Recommended Action	338
Severity	338
SEC-1097	338
Message	338
Probable Cause	338
Recommended Action	338
Severity	338
SEC-1098	338
Message	338
Probable Cause	338
Recommended Action	338
Severity	338
SEC-1099	338
Message	338
Probable Cause	338
Recommended Action	339
Severity	339
SEC-1100	339
Message	339
Probable Cause	339
Recommended Action	339
Severity	339
SEC-1101	339
Message	339
Probable Cause	339
Recommended Action	339
Severity	339
SEC-1102	339

Message	339
Probable Cause	340
Recommended Action	340
Severity	340
SEC-1104	340
Message	340
Probable Cause	340
Recommended Action	340
Severity	340
SEC-1105	340
Message	340
Probable Cause	340
Recommended Action	340
Severity	340
SEC-1106	341
Message	341
Probable Cause	341
Recommended Action	341
Severity	341
SEC-1107	341
Message	341
Probable Cause	341
Recommended Action	341
Severity	341
SEC-1108	341
Message	341
Probable Cause	341
Recommended Action	341
Severity	342
SEC-1110	342
Message	342
Probable Cause	342
Recommended Action	342
Severity	342
SEC-1111	342
Message	342
Probable Cause	342
Recommended Action	342
Severity	342
SEC-1112	342
Message	342
Probable Cause	342
Recommended Action	342
Severity	343
SEC-1115	343
Message	343
Probable Cause	343
Recommended Action	343
Severity	343
SEC-1116	343
Message	343
Probable Cause	343
Recommended Action	343
Severity	343
SEC-1117	343
Message	343
Probable Cause	343
Recommended Action	343
Severity	344

SEC-1118	344
Message	344
Probable Cause	344
Recommended Action	344
Severity	344
SEC-1119	344
Message	344
Probable Cause	344
Recommended Action	344
Severity	344
SEC-1121	344
Message	344
Probable Cause	344
Recommended Action	344
Severity	344
SEC-1122	345
Message	345
Probable Cause	345
Recommended Action	345
Severity	345
SEC-1123	345
Message	345
Probable Cause	345
Recommended Action	345
Severity	345
SEC-1124	345
Message	345
Probable Cause	345
Recommended Action	345
Severity	345
SEC-1126	346
Message	346
Probable Cause	346
Recommended Action	346
Severity	346
SEC-1130	346
Message	346
Probable Cause	346
Recommended Action	346
Severity	346
SEC-1135	346
Message	346
Probable Cause	346
Recommended Action	346
Severity	346
SEC-1136	347
Message	347
Probable Cause	347
Recommended Action	347
Severity	347
SEC-1137	347
Message	347
Probable Cause	347
Recommended Action	347
Severity	347
SEC-1138	347
Message	347
Probable Cause	348
Recommended Action	348

Severity	348
SEC-1139	348
Message	348
Probable Cause	348
Recommended Action	348
Severity	348
SEC-1142	348
Message	348
Probable Cause	348
Recommended Action	348
Severity	348
SEC-1145	349
Message	349
Probable Cause	349
Recommended Action	349
Severity	349
SEC-1146	349
Message	349
Probable Cause	349
Recommended Action	349
Severity	349
SEC-1153	349
Message	349
Probable Cause	349
Recommended Action	350
Severity	350
SEC-1154	350
Message	350
Probable Cause	350
Recommended Action	350
Severity	350
SEC-1155	350
Message	350
Probable Cause	350
Recommended Action	350
Severity	350
SEC-1156	351
Message	351
Probable Cause	351
Recommended Action	351
Severity	351
SEC-1157	351
Message	351
Probable Cause	351
Recommended Action	351
Severity	351
SEC-1158	351
Message	351
Probable Cause	351
Recommended Action	351
Severity	352
SEC-1159	352
Message	352
Probable Cause	352
Recommended Action	352
Severity	352
SEC-1160	352
Message	352
Probable Cause	352

Recommended Action	352
Severity	352
SEC-1163	352
Message	352
Probable Cause	352
Recommended Action	353
Severity	353
SEC-1164	353
Message	353
Probable Cause	353
Recommended Action	353
Severity	353
SEC-1165	353
Message	353
Probable Cause	353
Recommended Action	353
Severity	353
SEC-1166	353
Message	353
Probable Cause	353
Recommended Action	353
Severity	354
SEC-1167	354
Message	354
Probable Cause	354
Recommended Action	354
Severity	354
SEC-1168	354
Message	354
Probable Cause	354
Recommended Action	354
Severity	354
SEC-1170	354
Message	354
Probable Cause	354
Recommended Action	355
Severity	355
SEC-1171	355
Message	355
Probable Cause	355
Recommended Action	355
Severity	355
SEC-1172	355
Message	355
Probable Cause	355
Recommended Action	355
Severity	355
SEC-1173	355
Message	355
Probable Cause	356
Recommended Action	356
Severity	356
SEC-1174	356
Message	356
Probable Cause	356
Recommended Action	356
Severity	356
SEC-1175	356
Message	356

Probable Cause	356
Recommended Action	356
Severity	356
SEC-1176	356
Message	356
Probable Cause	356
Recommended Action	357
Severity	357
SEC-1180	357
Message	357
Probable Cause	357
Recommended Action	357
Severity	357
SEC-1181	357
Message	357
Probable Cause	357
Recommended Action	357
Severity	357
SEC-1182	357
Message	357
Probable Cause	357
Recommended Action	357
Severity	358
SEC-1183	358
Message	358
Probable Cause	358
Recommended Action	358
Severity	358
SEC-1184	358
Message	358
Probable Cause	358
Recommended Action	358
Severity	358
SEC-1185	358
Message	358
Probable Cause	358
Recommended Action	358
Severity	359
SEC-1186	359
Message	359
Probable Cause	359
Recommended Action	359
Severity	359
SEC-1187	359
Message	359
Probable Cause	359
Recommended Action	359
Severity	359
SEC-1188	359
Message	359
Probable Cause	359
Recommended Action	360
Severity	360
SEC-1189	360
Message	360
Probable Cause	360
Recommended Action	360
Severity	360
SEC-1190	360

Message	360
Probable Cause	360
Recommended Action	360
Severity	360
SEC-1191	361
Message	361
Probable Cause	361
Recommended Action	361
Severity	361
SEC-1192	361
Message	361
Probable Cause	361
Recommended Action	361
Severity	361
SEC-1193	361
Message	361
Probable Cause	361
Recommended Action	361
Severity	362
SEC-1194	362
Message	362
Probable Cause	362
Recommended Action	362
Severity	362
SEC-1195	362
Message	362
Probable Cause	362
Recommended Action	362
Severity	362
SEC-1196	362
Message	362
Probable Cause	362
Recommended Action	363
Severity	363
SEC-1197	363
Message	363
Probable Cause	363
Recommended Action	363
Severity	363
SEC-1198	363
Message	363
Probable Cause	363
Recommended Action	363
Severity	363
SEC-1199	363
Message	363
Probable Cause	364
Recommended Action	364
Severity	364
SEC-1200	364
Message	364
Probable Cause	364
Recommended Action	364
Severity	364
SEC-1201	364
Message	364
Probable Cause	364
Recommended Action	364
Severity	364

SEC-1202	365
Message	365
Probable Cause	365
Recommended Action	365
Severity	365
SEC-1250	365
Message	365
Probable Cause	365
Recommended Action	365
Severity	365
SEC-1251	365
Message	365
Probable Cause	365
Recommended Action	365
Severity	366
SEC-1253	366
Message	366
Probable Cause	366
Recommended Action	366
Severity	366
SEC-1300	366
Message	366
Probable Cause	366
Recommended Action	366
Severity	366
SEC-1301	366
Message	366
Probable Cause	366
Recommended Action	366
Severity	367
SEC-1302	367
Message	367
Probable Cause	367
Recommended Action	367
Severity	367
SEC-1303	367
Message	367
Probable Cause	367
Recommended Action	367
Severity	367
SEC-1304	367
Message	367
Probable Cause	367
Recommended Action	368
Severity	368
SEC-1305	368
Message	368
Probable Cause	368
Recommended Action	368
Severity	368
SEC-1306	368
Message	368
Probable Cause	368
Recommended Action	368
Severity	368
SEC-1307	368
Message	368
Probable Cause	369
Recommended Action	369

Severity	369
SEC-1308	369
Message	369
Probable Cause	369
Recommended Action	369
Severity	369
SEC-1309	369
Message	369
Probable Cause	369
Recommended Action	369
Severity	369
SEC-3001	369
Message	369
Probable Cause	370
Recommended Action	370
Severity	370
SEC-3002	370
Message	370
Probable Cause	370
Recommended Action	370
Severity	370
SEC-3003	370
Message	370
Probable Cause	370
Recommended Action	370
Severity	370
SEC-3004	371
Message	371
Probable Cause	371
Recommended Action	371
Severity	371
SEC-3005	371
Message	371
Probable Cause	371
Recommended Action	371
Severity	371
SEC-3006	371
Message	371
Probable Cause	371
Recommended Action	372
Severity	372
SEC-3007	372
Message	372
Probable Cause	372
Recommended Action	372
Severity	372
SEC-3008	372
Message	372
Probable Cause	372
Recommended Action	372
Severity	372
SEC-3009	372
Message	372
Probable Cause	373
Recommended Action	373
Severity	373
SEC-3010	373
Message	373
Probable Cause	373

Recommended Action	373
Severity	373
SEC-3011	373
Message	373
Probable Cause	373
Recommended Action	373
Severity	373
SEC-3012	374
Message	374
Probable Cause	374
Recommended Action	374
Severity	374
SEC-3013	374
Message	374
Probable Cause	374
Recommended Action	374
Severity	374
SEC-3014	374
Message	374
Probable Cause	374
Recommended Action	374
Severity	375
SEC-3015	375
Message	375
Probable Cause	375
Recommended Action	375
Severity	375
SEC-	375
Message	375
Probable Cause	375
Recommended Action	375
Severity	375
SEC-3017	375
Message	375
Probable Cause	375
Recommended Action	376
Severity	376
SNMP Error Messages	376
SNMP-1001	376
Message	376
Probable Cause	376
Recommended Action	376
Severity	376
SNMP-1002	376
Message	376
Probable Cause	376
Recommended Action	376
Severity	376
SNMP-1003	376
Message	376
Probable Cause	376
Recommended Action	377
Severity	377
SNMP-1004	377
Message	377
Probable Cause	377
Recommended Action	377
Severity	377
SS Error Messages	377

SS-1000	377
Message	377
Probable Cause	377
Recommended Action	377
Severity	377
SS-1001	377
Message	377
Probable Cause	377
Recommended Action	378
Severity	378
LB Error Messages	378
SULB-1001	378
Message	378
Probable Cause	378
Recommended Action	378
Severity	378
SULB-1002	378
Message	378
Probable Cause	378
Recommended Action	378
Severity	378
SULB-1003	378
Message	378
Probable Cause	379
Recommended Action	379
Severity	379
SULB-1005	379
Message	379
Probable Cause	379
Recommended Action	379
Severity	379
SULB-1006	379
Message	379
Probable Cause	379
Recommended Action	379
Severity	379
SULB-1007	379
Message	379
Probable Cause	380
Recommended Action	380
Severity	380
SULB-1008	380
Message	380
Probable Cause	380
Recommended Action	380
Severity	380
SULB-1009	380
Message	380
Probable Cause	380
Recommended Action	384
Severity	384
SULB-1010	384
Message	384
Probable Cause	384
Recommended Action	385
Severity	385
SWCH Error Messages	385
SWCH-1001	385
Message	385

Probable Cause	385
Recommended Action	385
Severity	385
SWCH-1002	385
Message	385
Probable Cause	385
Recommended Action	385
Severity	385
SWCH-1003	385
Message	385
Probable Cause	386
Recommended Action	386
Severity	386
SWCH-1004	386
Message	386
Probable Cause	386
Recommended Action	386
Severity	386
SWCH-1005	386
Message	386
Probable Cause	386
Recommended Action	386
Severity	386
SYSC Error Messages	387
SYSC-1001	387
Message	387
Probable Cause	387
Recommended Action	387
Severity	387
SYSC-1002	387
Message	387
Probable Cause	387
Recommended Action	387
Severity	387
SYSC-1003	387
Message	387
Probable Cause	388
Recommended Action	388
Severity	388
SYSM Error Messages	388
SYSM-1001	388
Message	388
Probable Cause	388
Recommended Action	388
Severity	388
SYSM-1002	388
Message	388
Probable Cause	388
Recommended Action	388
Severity	389
SYSM-1003	389
Message	389
Probable Cause	389
Recommended Action	389
Severity	389
SYSM-1004	389
Message	389
Probable Cause	389
Recommended Action	389

Severity	389
TRCE Error Messages	389
TRCE-1001	389
Message	389
Probable Cause	390
Recommended Action	390
Severity	390
TRCE-1002	390
Message	390
Probable Cause	390
Recommended Action	390
Severity	390
TRCE-1003	390
Message	390
Probable Cause	390
Recommended Action	390
Severity	391
TRCE-1004	391
Message	391
Probable Cause	391
Recommended Action	391
Severity	391
TRCE-1005	391
Message	391
Probable Cause	391
Recommended Action	391
Severity	391
TRCE-1006	391
Message	391
Probable Cause	392
Recommended Action	392
Severity	392
TRCE-1007	392
Message	392
Probable Cause	392
Recommended Action	392
Severity	392
TRCE-1008	392
Message	392
Probable Cause	392
Recommended Action	392
Severity	392
TRCE-1009	393
Message	393
Probable Cause	393
Recommended Action	393
Severity	393
TRCE-1010	393
Message	393
Probable Cause	393
Recommended Action	393
Severity	393
TRCE-1011	393
Message	393
Probable Cause	393
Recommended Action	393
Severity	394
TRCK Error Messages	394
TRCK-1001	394

Message	394
Probable Cause	394
Recommended Action	394
Severity	394
TRCK-1002	394
Message	394
Probable Cause	394
Recommended Action	394
Severity	394
TRCK-1003	394
Message	394
Probable Cause	394
Recommended Action	394
Severity	395
TRCK-1004	395
Message	395
Probable Cause	395
Recommended Action	395
Severity	395
TRCK-1005	395
Message	395
Probable Cause	395
Recommended Action	395
Severity	395
TRCK-1006	395
Message	395
Probable Cause	395
Recommended Action	395
Severity	395
TS Error Messages	396
TS-1001	396
Message	396
Probable Cause	396
Recommended Action	396
Severity	396
TS-1002	396
Message	396
Probable Cause	396
Recommended Action	396
Severity	396
TS-1006	397
Message	397
Probable Cause	397
Recommended Action	397
Severity	397
UCST Error Messages	397
UCST-1003	397
Message	397
Probable Cause	397
Recommended Action	397
Severity	397
UCST-1007	398
Message	398
Probable Cause	398
Recommended Action	398
Severity	398
UCST-1020	398
Message	398
Probable Cause	398

Recommended Action	398
Severity	398
UPTH Error Messages.	398
UPTH-1001	398
Message	398
Probable Cause	398
Recommended Action	398
Severity	399
USWD Error Messages.	399
USWD-1006	399
Message	399
Probable Cause	399
Recommended Action	399
Severity	399
WEBD Error Messages.	399
WEBD-1001	399
Message	399
Probable Cause	399
Recommended Action	399
Severity	399
WEBD-1002	399
Message	399
Probable Cause	399
Recommended Action	400
Severity	400
WEBD-1003	400
Message	400
Probable Cause	400
Recommended Action	400
Severity	400
WEBD-1004	400
Message	400
Probable Cause	400
Recommended Action	400
Severity	400
WEBD-1005	400
Message	400
Probable Cause	400
Recommended Action	400
Severity	401
WEBD-1006	401
Message	401
Probable Cause	401
Recommended Action	401
Severity	401
WEBD-1007	401
Message	401
Probable Cause	401
Recommended Action	401
Severity	401
ZOLB Error Messages.	401
ZOLB-1001	401
Message	401
Probable Cause	401
Recommended Action	401
Severity	402
ZONE Error Messages.	402
ZONE-1002	402
Message	402

Probable Cause	402
Recommended Action	402
Severity	402
ZONE-1003.	402
Message	402
Probable Cause	402
Recommended Action	402
Severity	402
ZONE-1004.	402
Message	402
Probable Cause	403
Recommended Action	403
Severity	403
ZONE-1005.	403
Message	403
Probable Cause	403
Recommended Action	403
Severity	403
ZONE-1006.	403
Message	403
Probable Cause	403
Recommended Action	404
Severity	404
ZONE-1007.	404
Message	404
Probable Cause	404
Recommended Action	404
Severity	404
ZONE-1008.	404
Message	404
Probable Cause	404
Recommended Action	404
Severity	404
ZONE-1010.	404
Message	404
Probable Cause	405
Recommended Action	405
Severity	405
ZONE-1012.	405
Message	405
Probable Cause	405
Recommended Action	405
Severity	405
ZONE-1013.	405
Message	405
Probable Cause	405
Recommended Action	405
Severity	405
ZONE-1014.	405
Message	405
Probable Cause	405
Recommended Action	406
Severity	406
ZONE-1015.	406
Message	406
Probable Cause	406
Recommended Action	406
Severity	406
ZONE-1017.	406

Message	406
Probable Cause	406
Recommended Action	406
Severity	406
ZONE-1018	406
Message	406
Probable Cause	407
Recommended Action	407
Severity	407
ZONE-1019	407
Message	407
Probable Cause	407
Recommended Action	407
Severity	407
ZONE-1022	407
Message	407
Probable Cause	407
Recommended Action	408
Severity	408
ZONE-1023	408
Message	408
Probable Cause	408
Recommended Action	408
Severity	408
ZONE-1024	408
Message	408
Probable Cause	408
Recommended Action	408
Severity	408
ZONE-1026	408
Message	408
Probable Cause	408
Recommended Action	408
Severity	409
ZONE-1027	409
Message	409
Probable Cause	409
Recommended Action	409
Severity	409
ZONE-1028	409
Message	409
Probable Cause	409
Recommended Action	409
Severity	409
ZONE-1029	410
Message	410
Probable Cause	410
Recommended Action	410
Severity	410
ZONE-1030	410
Message	410
Probable Cause	410
Recommended Action	410
Severity	410
ZONE-1031	410
Message	410
Probable Cause	410
Recommended Action	410
Severity	411

ZONE-1032.	411
Message	411
Probable Cause	411
Recommended Action	411
Severity	411
ZONE-1033.	411
Message	411
Probable Cause	411
Recommended Action	411
Severity	411
ZONE-1034.	411
Message	411
Probable Cause	411
Recommended Action	411
Severity	411
ZONE-1035.	412
Message	412
Probable Cause	412
Recommended Action	412
Severity	412
ZONE-1036.	412
Message	412
Probable Cause	412
Recommended Action	412
Severity	412
ZONE-1037.	412
Message	412
Probable Cause	412
Recommended Action	412
Severity	412
ZONE-1038.	413
Message	413
Probable Cause	413
Recommended Action	413
Severity	413
ZONE-1039.	413
Message	413
Probable Cause	413
Recommended Action	413
Severity	413
ZONE-1040.	413
Message	413
Probable Cause	413
Recommended Action	413
Severity	413
ZONE-1041.	414
Message	414
Probable Cause	414
Recommended Action	414
Severity	414
ZONE-3001.	414
Message	414
Probable Cause	414
Recommended Action	414
Severity	414
ZONE-3002.	414
Message	414
Probable Cause	414
Recommended Action	415

Severity	415
ZONE-3003	415
Message	415
Probable Cause	415
Recommended Action	415
Severity	415
ZONE-3004	415
Message	415
Probable Cause	415
Recommended Action	415
Severity	415
ZONE-3005	416
Message	416
Probable Cause	416
Recommended Action	416
Severity	416
ZONE-3006	416
Message	416
Probable Cause	416
Recommended Action	416
Severity	416
ZONE-3007	416
Message	416
Probable Cause	416
Recommended Action	416
Severity	417
ZONE-3008	417
Message	417
Probable Cause	417
Recommended Action	417
Severity	417
ZONE-3009	417
Message	417
Probable Cause	417
Recommended Action	417
Severity	417
ZONE-3010	417
Message	417
Probable Cause	417
Recommended Action	418
Severity	418
ZONE-3011	418
Message	418
Probable Cause	418
Recommended Action	418
Severity	418
ZONE-3012	418
Message	418
Probable Cause	418
Recommended Action	418
Severity	418

Index	419
-----------------	-----

Tables

1 Document conventions	78
2 Commands used to view or configure the system logs	84
3 Error message field description	86
4 System module descriptions	89

5	Upgrade messages and code values	381
6	Upgrade state and code value	384

About this guide

This installation guide provides information about:

- Understanding system error messages
- Troubleshooting system error messages
- Switch diagnostics

Intended audience

This guide is intended for:

- system administrators responsible for setting up HP StorageWorks Fibre Channel Storage Area Network (SAN) switches
- technicians responsible for maintaining the Fabric Operating System (OS)

Related documentation

Documentation, including white papers and best practices documents, is available on the HP web site:

<http://www.hp.com/country/us/eng/prodserv/storage.html>

To access current Fabric OS 5.x related documents:

1. Locate the **IT storage Products** section of the web page.
2. Under **Networked storage**, click **SAN Infrastructure**.
3. From the **SAN Infrastructure** web page, locate the **SAN Infrastructure products** section.
4. Click **Fibre Channel Switches**.
5. Locate the B-Series-Fabric-Enterprise Class section.
6. To access Fabric OS 5.x documents (such as this document), click **4/256 SAN Director and 4/256 SAN Director power pack**.

The switch overview page displays.

7. Go to the **Product Information section**, located on the right side of the web page.
8. Click **Technical documents**.
9. Follow the onscreen instructions to download the applicable documents.


Document conventions and symbols


Table 1 Document conventions

Convention	Element
Medium blue text: Figure 1	Cross-reference links and e-mail addresses
Medium blue, underlined text (http://www.hp.com)	Web site addresses
Bold font	<ul style="list-style-type: none">• Key names• Text typed into a GUI element, such as into a box• GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes
<i>Italics font</i>	Text emphasis
Monospace font	<ul style="list-style-type: none">• File and directory names• System output• Code• Text typed at the command-line
<i>Monospace, italic font</i>	<ul style="list-style-type: none">• Code variables• Command-line variables
Monospace, bold font	Emphasis of file and directory names, system output, code, and text typed at the command line

 **WARNING!** Indicates that failure to follow directions could result in bodily harm or death.

 **CAUTION:** Indicates that failure to follow directions could result in damage to equipment or data.

 **IMPORTANT:** Provides clarifying information or specific instructions.

 **NOTE:** Provides additional information.

 **TIP:** Provides helpful hints and shortcuts.

HP technical support

Telephone numbers for worldwide technical support are listed on the HP support web site:
<http://www.hp.com/support/>.

Collect the following information before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

For continuous quality improvement, calls may be recorded or monitored.

HP strongly recommends that customers sign up online using the Subscriber's choice web site:
<http://www.hp.com/go/e-updates>.

- Subscribing to this service provides you with e-mail updates on the latest product enhancements, newest versions of drivers, and firmware documentation updates as well as instant access to numerous other product resources.
- After signing up, you can quickly locate your products by selecting **Business support** and then **Storage** under Product Category.

HP-authorized reseller

For the name of your nearest HP-authorized reseller:

- In the United States, call 1-800-282-6672.
- Elsewhere, visit the HP web site: <http://www.hp.com>. Then click **Contact HP** to find locations and telephone numbers.

Helpful web sites

For other product information, see the following HP web sites:

- <http://www.hp.com>
- <http://www.hp.com/go/storage>
- <http://www.hp.com/support/>
- <http://www.docs.hp.com>

1 Introduction to System Messages

This guide supports Fabric OS 5.x and contains system messages that you can use to diagnose and fix problems with the switch or fabric. The messages are organized alphabetically by module name. A *module* is a subsystem in the Fabric OS. Each module generates a set of numbered messages. For each message, this book provides message text, probable cause, recommended action, and severity level. There can be more than one cause and more than one recommended action for any given message. This guide discusses the most probable cause and typical action recommended.

This chapter provides an introduction to the system messages. The following topics are discussed:

- [Message severity levels](#), page 81
- [Overview of the system messages](#), page 81
- [View or configure the system message logs](#), page 84
- [Reading a system message](#), page 85
- [Responding to a system message](#), page 88
- [System module descriptions](#), page 89

Message severity levels

There are four levels of severity for messages, ranging from Critical (1) to Info (4). In general, the definitions are wide ranging and are to be used as general guidelines for troubleshooting. For all cases, you should look at each specific error message description thoroughly before taking action. System messages have the following severity levels.

1 = CRITICAL	Critical-level messages indicate that the software has detected serious problems that will cause a partial or complete failure of a subsystem if not corrected immediately; for example, a power supply failure or rise in temperature must receive immediate attention.
2 = ERROR	Error-level messages represent an error condition that does not impact overall system functionality significantly. For example, error-level messages might indicate time-outs on certain operations, failures of certain operations after retries, invalid parameters, or failure to perform a requested operation.
3 = WARNING	Warning-level messages highlight a current operating condition that should be checked or it might lead to a failure in the future. For example, a power supply failure in a redundant system relays a warning that the system is no longer operating in redundant mode unless the failed power supply is replaced or fixed.
4 = INFO	Info-level messages report the current non-error status of the system components: for example, detecting online and offline status of a fabric port.

Overview of the system messages

This section provides information on the various logs saved by the system and how to view the information in the log files, including the following topics:

- [System message log \(RASLog\)](#), page 82
- [Audit logging](#), page 82
- [Dual-CP systems](#), page 83
- ["System logging daemon"](#) on page 83
- [Port logs](#), page 83
- [Panic dump and core dump files](#), page 83
- [Trace dumps](#), page 84
- [supportSave command](#), page 84

- [System console](#), page 84

System message log (RASLog)

The Fabric OS maintains an internal system message log of all messages. For Fabric OS 5.x, this log is saved as a RASLog. Features of the system message log include the following:

- The system message log by default saves all messages to nonvolatile storage.
- The system message log can save a maximum of 1024 messages in RAM.
- The system message log is implemented as a circular buffer. When more than maximum entries are added to the log file, old entries are overwritten by new entries.
- Messages are numbered sequentially from 1 to 2,147,483,647 (0x7fffffff). The sequence number will continue to increase beyond the storage limit of 1024 messages. The sequence number can be reset to 1 using the **errClear** command. The sequence number is persistent across power cycles and switch reboots.
- By default, the **errDump** and **errShow** commands display all of the system messages.
- You should configure the syslogd facility as a management tool for error logs. This is particularly important for dual-domain switches, as the syslogd facility saves messages from two CPs as a single file and in sequential order. See ["System logging daemon"](#) on page -83 for more information.

Audit logging

Audit messages are enhanced to record more information, for security purposes. They are flagged AUDIT in the system message log. Currently, the only messages that have the audit flag set are SEC-3001 to SEC-3017 and ZONE-3001 to ZONE-3012.

They provide the following information:

- User Name: The name of the user who triggered the action.
 - Role: The role of the user: for example, root or admin.
 - Event Name: The name of the event that occurred.
 - Status: The status of the event that occurred: success or failure.
 - Event Info: Information about the event.
- If you are creating an SCC_POLICY and use wildcards such as the asterisk (*), meaning all the switches in the current fabric, these wildcards are displayed in the audit error message.

An example audit message is as follows:

```
2004/07/09-02:09:40, [SEC-3001], 181, AUDIT, INFO, User:rick, role: admin, Event:
secpolicy create, status:success, Info: Create SCC_POLICY policy, with * entries.
```

Only certain commands generate an AUDIT message in the system message log.

The commands that generate SEC AUDIT messages are as follows:

- **secModeEnable** and **secModeDisable**
- **secPolicyCreate**, **secPolicyDelete**, **secPolicyRemove**, **secPolicyActivate**, and **secPolicySave**
- **login** and **logout**
- **secFCSFailover**
- **secTransAbort**
- **secStatsReset**
- **secTempPasswdSet** and **secTempPasswdReset**
- **aaaConfig**
- **authUtil**

The commands that generate ZONE AUDIT messages are as follows:

- **cfgEnable**
- **cfgDisable**
- **cfgSave**

- `cfgTransAbort`
- `zoneObjectCopy`
- `zoneObjectExpunge`
- `zoneObjectRename`

Dual-CP systems

For the *Core Switch 2/64*, *SAN Director 2/128*, and *4/256 SAN Director*, each CP has a unique error log, depending on which CP was active when that message was reported. To fully understand message logging on these switches, you should enable the system logging daemon because the logs on the host computer are maintained in a single merged file for both CPs and are in sequential order. Otherwise, you must examine the error logs in both CPs, particularly for events such as **firmwareDownload** or **haFailover**, for which the active CP changes.

For the security violations such as telnet, HTTP, and serial connection violations are not propagated between CPs. Security violations on the active CP are not propagated to the standby CP counters in the event of a failover, nor do security violations on the standby CP get propagated to the active CP counters.

System logging daemon

The system logging daemon (syslogd) is a process on UNIX, Linux, and some Windows systems that reads and logs messages as specified by the system administrator.

Fabric OS can be configured to use a UNIX-style syslogd process to forward system events and error messages to log files on a remote host system.

The host system can be running UNIX, Linux, or any other operating system that supports the standard syslogd functionality.

Configuring for syslogd involves configuring the host, enabling syslogd on the SilkWorm model, and, optionally, setting the facility level.

For information on configuring syslogd functionality, refer to the *Fabric OS Administrator's Guide*.

Port logs

The Fabric OS maintains an internal log of all port activity. Each switch or logical switch maintains a log file for each port. Port logs are circular buffers that can save up to 8000 entries per logical switch. When the log is full, the newest log entries overwrite the oldest log entries. Port logs capture switch-to-device, device-to-switch, switch-to-switch, some device A-to-device B, and control information. Port logs are not persistent and are lost over power cycles and reboots.

Run the **portLogShow** command to display the port logs for a particular port.

Run the **portLogEventShow** command to display the specific events reported for each port.

Refer to the *Fabric OS Administrator's Guide* for information on interpreting results of the **portLogDump** command.

Port log functionality is completely separate from the system message log. Port logs are typically used to troubleshoot device connections.

Panic dump and core dump files

The Fabric OS creates panic dump files and core files when there are problems in the Fabric OS kernel. These files can build up in the kernel partition (typically because of failovers) and might need to be periodically deleted or downloaded using the **saveCore** command. In case of a panic dump, the files can be viewed with the **pdShow** command.

The software watchdog process (SWD) is responsible for monitoring daemons critical to the function of a healthy switch. The SWD holds a list of critical daemons that ping the SWD periodically at a predetermined interval defined for each daemon.

If a daemon fails to ping the SWD within the defined interval, or if the daemon terminates unexpectedly, then the SWD dumps information to the panic dump files, which helps to diagnose the root cause of the unexpected failure.

Run the **pdShow** command to view these files or the **saveCore** command to send them to a host workstation using FTP. The panic dump files and core files are intended for support personnel use only.

Trace dumps

The Fabric OS produces trace dumps when problems are encountered within Fabric OS modules. You can initiate the sending of trace dump files to support personnel using the **supportSave** or **traceFtp** command. The Fabric OS trace dumps files are intended for support personnel use only.

supportSave command

The **supportSave** command can be used to send by FTP the output of the system messages (RASLog), the trace files, and the output of the **supportShow** command to a support location. Prior to running the **supportSave** command, you can optionally set up the FTP parameters using the **supportFtp** command. The **supportShow** command runs a large number of dump and show commands to provide a global output of the status of the switch. Refer to the *HP StorageWorks Fabric OS 5.x command reference guide* for more information on these commands.

System console

The system console displays messages only through the serial port. If you log in to a switch through the Ethernet port or modem port, you will not receive system console messages.

The **errFilterSet** command can be used by administrators to filter messages that appear on the system console by severity. All messages are still sent to the system message log and syslog (if enabled).

The system console displays both system messages and panic dump messages. These messages are mirrored to the system console; they are always saved in one of the system logs.

View or configure the system message logs

Table 2 lists commands that are used to view or configure the system message logs. Many of these commands require admin login privileges in order to execute.

Table 2 Commands used to view or configure the system logs

Command	Description
agtCfgDefault	Resets the SNMP recipients to default values.
agtCfgSet	Configures the SNMP recipients.
agtCfgShow	Displays the current configuration of the SNMP recipients.
errClear	Clears the error log.
errDelimiterSet	Sets the error log start and end delimiter for messages pushed to the console.
errDump	Displays the entire error log, without page breaks. Use the -r option to show the messages in reverse order, from newest to oldest.
errFilterSet	Sets an error severity filter for the system console.
errShow	Displays the entire error log, with page breaks. Use the -r option to show the messages in reverse order, from newest to oldest.
pdShow	Displays the contents of the panic dump and core dump files.
portErrShow	Displays the port error summary.
portLogClear	Clears the port log. (If the port log is disabled, this commands enables it.)
portLogDisable	Disables the port log facility.
portLogDump	Displays the port log, without page breaks.
portLogDumpPort	Displays the port log of the specified port, without page breaks.

Table 2 Commands used to view or configure the system logs (continued)

Command	Description
portLogEventShow	Displays which port log events are currently being reported.
portLoginShow	Displays port logins.
portLogPdisc	Sets or clear the debug pdisc_flag.
portLogReset	Enables the port log facility.
portLogResize	Resizes the port log to the specified number of entries.
portLogShow	Displays the port log, with page breaks.
portLogShowPort	Displays the port log of a port, with page breaks for a specific port.
portLogTypeDisable	Disables an event from reporting to the port log. Port log events are described by the portLogEventShow command.
portLogTypeEnable	Enables an event to report to the port log. Port log events are described by the portLogEventShow command.
saveCore	Saves or removes core files created by the kernel.
setVerbose	Sets the verbose level of a particular module within the Fabric OS.
supportFtp	Sets, clears, or displays support FTP parameters or a time interval to check the FTP server.
supportSave	Collects RASLog, trace files, and supportShow (active CP only) information for the local CP and then transfers the files to an FTP server. The operation can take several minutes.
supportShow	Executes a list of diagnostic and error display commands. This output is used by your switch service provider to diagnose and correct problems with the switch. The output from this command is very long.
syslogDIpAdd	Adds an IP address as a recipient of system messages.
syslogDIpRemove	Removes an IP address as a recipient of system messages.
syslogDIpShow	Views the currently configured IP addresses that are recipients of system messages.
syslogdFacility	Changes the syslogd facility.
traceDump	Displays, initiates, or removes a Fabric OS module trace dump.
traceFtp	Displays, enables, or disables the trace auto-FTP or retrieves the trace dump file.
traceTrig	Sets, removes, or displays trace triggers.

Reading a system message

This section provides information about reading system messages.

Example system message

The following example shows a sample message from the error log:

```
2004/07/22-10:12:33, [EM-1031], 4,, ERROR, switchname, Slot 7
ejector not closed
```

The fields in the error message are described in table below.

Table 3 Error message field description

Example	Variable Name	Description
2004/07/22-10:12:33	Date and Time Stamp	The system time (UTC) when the message was generated on the switch. The RASLog subsystem will support an internationalized timestamp format base on the "LOCAL" setting.
[EM-1031]	Message Module and Message Number	Displays the message module and number. These values uniquely identify each message in the Fabric OS and are used to reference the cause and actions in this manual. Note that not all message numbers are used and there can be gaps in the numbering of messages.
4	Sequence Number	<p>This represents the error message position in the log. When any messages are added to the log, this number is incremented. When this message reaches the last position in the error log, and becomes the oldest message in the log, it is deleted when a new message is added.</p> <p>In Fabric OS 5.x, the message sequence number starts at 1 after a firmwareDownload and will increase up to a value of 2,147,483,647 (0x7ffffff).</p> <p>The sequence number will continue to increase beyond the storage limit of 1024 messages. The sequence number can be reset to 1 using the errClear command. The sequence number is persistent across power cycles and switch reboots.</p>
, <AUDIT>, (not shown in the above example)	Audit Flag	Indicates that this message is an AUDIT message for a security issue. The only messages that have the audit flag set are SEC-3001 through SEC-3017. For all other messages, this field is blank; however, the commas still appear, so many messages have two commas separated by a blank space.
ERROR	Severity Level	<p>Displays the severity of the error in alpha format:</p> <p>1 = Critical 2 = Error 3 = Warning 4 = Info</p>

Table 3 Error message field description (continued)

Example	Variable Name	Description
switchname	Switch name or chassis name, depending on the action; for example, HA messages typically show the chassis name and login failures show the logical switch name.	This field displays the defined switch name or the chassis name of the switch. This value is truncated if it is over 16 characters in length. Run either the chassisName command to name the chassis or the switchName command to rename the logical switch.
Slot 7 ejector not closed	Error Description	This field displays a text string explaining the error encountered and providing parameters supplied by the software at runtime.

Viewing system messages from AdvancedWeb Tools

This procedure is valid for HP StorageWorks Fabric OS 5.x switches.

To view the system message log for a switch from Advanced Web Tools:

1. Launch Web Tools.
2. Select the desired switch from the Fabric Tree. The Switch View displays.
3. Click the **Switch Events** button. A Switch Events Report appears.
4. View the switch events and messages. In dual-domain switches, an Event button exists for each logical switch. Only messages relating to that switch (and chassis) will be displayed.

Dumping the system messages

This procedure is valid for the HP StorageWorks Fabric OS 5.x switches.

To display the system message log, with no page breaks:

1. Log in to the switch as admin.
2. Enter the **errDump** command at the command line:

```
switch:admin> errDump
Version: 5.0.1
2004/07/28-17:04:59, [FSSM-1002], 1,, INFO, switch, HA State is in
sync

2004/07/28-17:04:59, [FSSM-1003], 2,, WARNING, switch, HA State out
of sync

2004/07/28-17:04:51, [EM-1055], 3,, WARNING, switch, Media 27: Port
media incompatible. Reason: Configured port speed.

2004/07/28-17:04:54, [FABR-1001], 4,, WARNING, switch, port 4, ELP
rejected by the other switch

2004/07/28-17:05:06, [FW-1050], 5,, WARNING, switch, Sfp Supply
Voltage 0, is below low boundary(High=3600, Low=3150). Current value
is 0 mV.

switch:admin>
```

Viewing the system messages with page breaks

This procedure is valid for HP StorageWorks Fabric OS 5.x switches.

To display the system message log, with page breaks:

1. Log in to the switch as admin.
2. At the command line, enter the **errShow** command:

```
switch:admin> errShow
Version: 5.0.1
2004/07/28-17:04:59, [FSSM-1002], 1,, INFO, switch, HA State is in
sync

Type <CR> to continue, Q<CR> to stop:

2004/07/28-17:04:59, [FSSM-1003], 2,, WARNING, switch, HA State out
of sync

Type <CR> to continue, Q<CR> to stop:

2004/07/28-17:04:51, [EM-1055], 3,, WARNING, switch, Media 27: Port
media incompatibl
e. Reason: Configured port speed.

Type <CR> to continue, Q<CR> to stop:
```

Clearing the system message log

This procedure is valid for HP StorageWorks Fabric OS 5.x switches.

To clear the system message log for a particular switch instance:

1. Log in to the switch as admin.
2. Enter the **errClear** command to clear all messages from memory

The following example shows how to clear the system message log:

```
switch:admin> errclear
switch:admin>
```

Responding to a system message

This section provides procedures on gathering information on system messages.

Looking up a system message

Error messages are arranged in this manual alphabetically. To look up an error message, copy down the appropriate module number and the error code and compare this with the Table of Contents to determine the location of the information for that error message.

Information provided by this book is as follows:

- Module and code name for the error
- Message text
- Probable cause
- Recommended action
- Message severity

Gathering information

Common steps and questions to ask yourself when troubleshooting a system message are as follows:

1. What is the current Fabric OS level?
2. What is the switch hardware version?
3. Is the switch operational?
4. Assess impact and urgency:
 - Is the switch down?
 - Is it a standalone switch?
 - How large is the fabric?
 - Is the fabric redundant?
5. Run the **errDump** command on each logical switch.
6. Run **supportFtp** (as needed) to set up automatic FTP transfers, and then run the **supportSave** command.
7. Document the sequence of events by answering the following questions:
 - What happened just prior to the problem?
 - Is the problem repeatable?
 - If so, what are the steps to produce the problem?
 - What configuration was in place when the problem occurred?
8. Did a failover occur?
9. Was security enabled?
10. Was POST enabled?
11. Are serial port (console) logs available?
12. Which CP was master? (only applicable to the)
13. What and when were the last actions or changes made to the system?

System module descriptions

<Link>Table 4 provides a summary of the system modules for which messages are documented in this reference guide; the system modules are listed alphabetically by name.

Table 4 System module descriptions

System module	Description
AUTH	Authentication error messages indicate problems with the authentication module of the Fabric OS.
BL	Blade error messages are a result of faulty hardware, transient out-of-memory conditions, ASIC errors, or inconsistencies in the software state between a blade and the EM (environment monitor) module.
BLL	Bloom is the name of the ASIC used as the building block for third-generation hardware platforms.
CER	This is the core edge routing module on the SilkWorm director platforms.

Table 4 System module descriptions (continued)

System module	Description
EM	<p>The environmental monitor (EM) manages and monitors the various FRUs (field replaceable units), including the port cards, CP blades, blower assemblies, power supplies, and WWN (World Wide Name) cards. EM controls the state of the FRUs during system startup, hot-plug sequences, and fault recovery.</p> <p>EM provides access to and monitors the sensor and status data from the FRUs and maintains the integrity of the system using the environmental and power policies. EM reflects system status by way of telnet commands, system LEDs, and status and alarm messages. EM also manages some component-related data.</p>
EVMD	This is the event management module.
FABR	FABRIC refers to a network of Fibre Channel switches. The FABRIC error messages come from the fabric daemon. The fabric daemon follows the FC-SW-3 standard for the fabric initialization process, such as determining the E_Ports, assigning unique domain IDs to switches, creating a spanning tree, throttling the trunking process, and distributing the domain and alias lists to all switches in the fabric.
FABS	Fabric OS system driver module.
FCMC	Fibre Channel miscellaneous messages relate to problems with the physical layer used to send Fibre Channel traffic to and from the switch.
FCPD	The Fibre Channel Protocol daemon is responsible for probing the devices attached to the loop port. Probing is a process the switch uses to find the devices attached to the loop ports and to update the Name Server with the information.
FCPH	Fibre Channel Physical Layer is used to send Fibre Channel traffic to and from the switch.
FICU	The FICON-CUP daemon handles communication with FICON on IBM FICON storage devices. Errors to this module are usually initiation errors or indications that FICON-CUP prerequisites have not been met, such as a license key, core PID, and secure mode on the fabric.
FKLB	Fabric OS I/O kernel library module.
FLOD	FLOOD is a part of the FSPF (fabric shortest path first) protocol that handles synchronization of the link state database (LSDB) and propagation of the link state records (LSR).
FSPF	Fabric shortest path first (FSPF) is a link state routing protocol that is used to determine how frames should be routed. These messages are about protocol errors.
FSS	<p>The Fabric OS state synchronization framework provides facilities by which the active control processor (CP) can synchronize with the standby CP, enabling the standby CP to take control of the switch nondisruptively during failures and software upgrades. These facilities include version negotiation, state information transfer, and internal synchronization functions, enabling the transition from standby to active operation.</p> <p>FSS is defined both as a component and a service. A <i>component</i> is a module in the Fabric OS, implementing a related set of functionality. A <i>service</i> is a collection of components grouped together to achieve a modular software architecture.</p>

Table 4 System module descriptions (continued)

System module	Description
FSSM	The Fabric OS state synchronization management module is defined both as a component and a service. A component is a module in Fabric OS implementing a related set of functionality. A service is a collection of components grouped together to achieve a modular software architecture.
FW	FW is the Fabric Watch module. This module monitors thresholds for many switch subsystems: for example, temperature, voltage, fan speed, and switch status. Any changes that cross a specified threshold are reported to the system message log.
HAM	HAM is a user space daemon responsible for high availability management.
HAMK	This is the kernel module for the HAM daemon.
HIL	Hardware independent layer.
HLO	HLO is a part of FSPF protocol that handles the HELLO protocol between adjacent switches. The HELLO protocol is used to establish connectivity with a neighbor switch, to establish the identity of the neighbor switch, and to exchange FSPF parameters and capabilities.
HMON	Health monitor.
HTTP	HTTP error message.
KSWD	<ul style="list-style-type: none"> • The kernel software watchdog (KSWD) watches daemons for unexpected terminations and “hang” conditions and informs the HAM module to take corrective actions such as failover or reboot. • The following daemons are monitored by KSWD: • Diagnostics daemon (DIAGD) • Environment monitor daemon (EMD) • EVM daemon (EVMD) • Fabric daemon (FABRICD) • FCPD daemon (FCPD) • FDMI daemon (FDMID) • FICON-CUP daemon (FICUD) • FSPF daemon (FSPFD) • Fabric watch daemon (FWD) • Management Server daemon (MSD) • Name Server daemon (NSD) • PDM daemon (PDMD) • PS daemon (PSD) • Reliable commit service daemon (RCSD) • FA-API RPC daemon (RPCD) • Security daemon (SECD) • SNMP daemon (SNMPD) • Track changes daemon (TRACK_CHANGES) • Time Service daemon (TSD) • Web Tools daemon (WEBD) • Zone daemon (ZONED)

Table 4 System module descriptions (continued)

System module	Description
KTRC	<ul style="list-style-type: none"> Kernel RAS trace module.
LOG	<ul style="list-style-type: none"> RASLog subsystem.
LSDB	<ul style="list-style-type: none"> The link state database is a part of the FSPF protocol that maintains records on the status of port links. This database is used to route frames.
MFIC	<ul style="list-style-type: none"> MS-FICON messages relate to FICON installations. FICON-CUP messages are displayed under the FICU module.
MPTH	<ul style="list-style-type: none"> Multicast path uses the shortest path first (SPF) algorithm to dynamically compute a broadcast tree.
MQ	<ul style="list-style-type: none"> Message queues are used for interprocess communication. Message queues allow many messages, each of variable length, to be queued. Any process or interrupt service routine (ISR) can write messages to a message queue. Any process can read messages from a message queue.
MS	<ul style="list-style-type: none"> The Management Service enables the user to obtain information about the Fibre Channel fabric topology and attributes by providing a single management access point. MS provides for both monitoring and control of the following areas: <ul style="list-style-type: none"> Fabric Configuration Server. Provides for the configuration management of the fabric. Unzoned Name Server. Provides access to Name Server information that is not subject to zone constraints. Fabric Zone Server. Provides access to and control of zone information.
NBFS	<ul style="list-style-type: none"> NBFSM is a part of the FSPF (fabric shortest path first) protocol that handles a neighboring or adjacent switch's finite state machine (FSM). Input to the FSM changes the local switch from one state to another, based on specific events. For example, when two switches are connected to each other using an ISL (interswitch link) cable, they are in the Init state. After both switches receive HELLO messages, they move to the Database Exchange state, and so on. NBFSM states are Down (0), Init (1), Database Exchange (2), Database Acknowledge Wait (3), Database Wait (4), and Full (5).
NS	Indicates problems with the Simple Name Server module.
PDM	Parity data manager is a user space daemon responsible for the replication of persistent configuration files from the primary partition to the secondary partition and from the active CP blade to the standby CP blade.
PDTR	These messages indicate panic dump trace files have been created.
PLAT	This message indicates hardware problems.
PORT	PORT error messages refer to the front-end user ports on the switch. Front-end user ports are directly accessible by users, to connect end devices or connect to other switches.
PS	The performance server daemon measures the amount of traffic between end points or traffic with particular frame formats, such as SCSI frames, IP frames, and customer-defined frames.

Table 4 System module descriptions (continued)

System module	Description
PSWP	The portswap feature and associated commands generate these error messages.
RCS	The reliable commit service daemon generates log entries when it receives a request from the zoning, security, or management server for passing data messages to switches in the fabric. RCS then requests RTWR (reliable transport write and read) to deliver the message. RCS also acts as a gatekeeper, limiting the number of outstanding requests for the Zoning, Security, or Management Server modules.
RPCD	The remote procedure call daemon (RPCD) is used by Fabric Access for API-related tasks.
RTWR	The reliable transport write and read daemon helps deliver data messages either to specific switches in the fabric or to all of the switches in the fabric. For example, if some of the switches are not reachable or are offline, RTWR returns an “unreachable” message to the caller, allowing the caller to take the appropriate action. If a switch is not responding, RTWR retries 100 times.
SCN	The internal state change notification daemon is used for state change notifications from the kernel to the daemons within Fabric OS.
SEC	The security daemon generates security errors, warnings, or information during security-related data management or fabric merge operations. Administrators should watch for these messages, to distinguish between internal switch and fabric operation errors, and external attack.
SNMP	Simple Network Management Protocol is a universally supported low-level protocol that allows simple get, get next, and set requests to go to the switch (acting as an SNMP agent). It also allows the switch to send traps to the defined and configured management station. Brocade switches support six management entities that can be configured to receive these traps.
SS	The supportSave command generates these error messages if problems are encountered.
SULB	The software upgrade library provides firmwareDownload command capability, which enables firmware upgrades to both CP blades with a single command, as well as nondisruptive code load to all 4.x switches. These messages might display if there are any problems during the firmwareDownload procedure. Most messages are informational only and are generated even during successful firmware download. For additional information, refer to the <i>Fabric OS Administrator’s Guide</i> .
SWCH	These messages are generated by the switch driver module that manages a Fibre Channel switch instance.
SYSC	System controller is a daemon that starts up and shuts down all Fabric OS modules in the proper sequence.
YSYM	General system messages.
TRCE	RAS TRACE error messages.

Table 4 System module descriptions (continued)

System module	Description
TRCK	<p>The track change feature tracks the following events:</p> <ul style="list-style-type: none">• Turning on or off the track change feature• CONFIG_CHANGE• LOGIN• LOGOUT• FAILED_LOGIN <p>If any of these events occurs, a message is sent to the system message log. Additionally, if the SNMP trap option is enabled, an SNMP trap is also sent.</p> <p>For information on configuring the track change feature, refer to the <i>HP StorageWorks Fabric OS 5.x command reference guide</i> or the <i>Fabric OS Administrator's Guide</i>.</p>
TS	Time Service provides fabric time-synchronization by synchronizing all clocks in the fabric to the clock time on the principal switch.
UCST	UCAST is a part of the fabric shortest path first (FSPF) protocol that manages the Unicast routing table.
UPTH	UPATH is a part of the FSPF protocol that uses the SPF algorithm to dynamically compute a Unicast tree.
USWD	The user-space software watchdog daemon informs the KSWD about which daemons the watchdog subsystem will monitor. Additionally, the USWD daemon helps the KSWD daemon to print debug information if a critical daemon has an unexpected termination.
WEBD	Indicates problems with the Web Tools module.
ZOLB	Indicates problems with the zone library module.
ZONE	The zone module messages indicate any problems associated with the zoning features, including commands associated with aliases, zones, and configurations.

2 Error messages

AUTH error messages

AUTH-1001

Message

```
<timestamp>, [AUTH-1001], <sequence-number>,, INFO, <system-name>,  
<Operation type> has been successfully done.
```

Probable Cause

Indicates that the secret database operation has been updated using the **secAuthSecret** command. The values for Operation type can be "set" or "remove".

Recommended Action

No action is required.

Severity

INFO

Message

```
<timestamp>, [AUTH-1002], <sequence-number>,, ERROR, <system-name>,  
<Operation type> has failed.
```

Probable Cause

Indicates that the specified action has failed to update the secret database using the **secAuthSecret** command. The values for Operation type can be "set" or "remove".

Recommended Action

Retry the **secAuthSecret** command.

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

AUTH-1003

Message

```
<timestamp>, [AUTH-1003], <sequence-number>,, INFO, <system-name>,  
<data type> type has been successfully set to <setting value>.
```

Probable Cause

Indicates an authentication configuration value was set to a specified value. The data type is either authentication type or DH group type.

Recommended Action

No action is required.

Severity

INFO

AUTH-1004

Message

```
<timestamp>, [AUTH-1004], <sequence-number>,, ERROR, <system-name>,  
Failed to set <data type> type to <setting value>.
```

Probable Cause

Indicates that the **authUtil** command has failed to set the authentication configuration value. The data type can be either authentication type or DH group type.

Recommended Action

Retry the **authUtil** command.

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

AUTH-1005

Message

```
<timestamp>, [AUTH-1005], <sequence-number>,, ERROR, <system-name>,  
Authentication file does not exist: <error code>.
```

Probable Cause

Indicates an authentication file corruption.

Recommended Action

Run the **firmwareDownload** command to reinstall the firmware.

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

AUTH-1006

Message

```
<timestamp>, [AUTH-1006], <sequence-number>,, ERROR, <system-name>,  
Failed to open authentication configuration file.
```

Probable Cause

Indicates an internal problem with the Secure Fabric OS.

Recommended Action

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

AUTH-1007

Message

```
<timestamp>, [AUTH-1007], <sequence-number>,, ERROR, <system-name>,  
The proposed authentication protocol(s) are not supported: port  
<port number>.
```

Probable Cause

Indicates that the proposed authentication protocol type or types are not supported by the local port.

Recommended Action

Run the **authUtil** command to make sure the local switch supports the specified protocols: FCAP or DH-CHAP.

Severity

ERROR

AUTH-1008

Message

```
<timestamp>, [AUTH-1008], <sequence-number>,, ERROR, <system-name>,  
No security license, operation failed.
```

Probable Cause

Indicates that the switch does not have a security license.

Recommended Action

Verify that the security license is installed using the **licenseShow** command. If necessary, reinstall the license using the **licenseAdd** command.

Severity

ERROR

AUTH-1010

Message

```
<timestamp>, [AUTH-1010], <sequence-number>,, ERROR, <system-name>,  
Failed to initialize security policy: switch <switch number>, error  
<error code>.
```

Probable Cause

Indicates an internal problem with the Secure Fabric OS.

Recommended Action

Reboot or power cycle the switch.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

AUTH-1011

Message

```
<timestamp>, [AUTH-1011], <sequence-number>,, ERROR, <system-name>,  
Failed to register for failover operation: switch <switch number>  
error <error code>
```

Probable Cause

Indicates an internal problem with the Secure Fabric OS.

Recommended Action

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

AUTH-1012

Message

```
<timestamp>, [AUTH-1012], <sequence-number>,, WARNING,  
<system-name>, Authentication <code> is rejected: port <port  
number> explain <explain code> reason <reason code>
```

Probable Cause

Indicates that an authentication is rejected because the remote entity does not support authentication.

Recommended Action

Make sure the entity at the other end of the link supports authentication.

Severity

WARNING

AUTH-1013

Message

```
<timestamp>, [AUTH-1013], <sequence-number>,, WARNING,  
<system-name>, Can not perform authentication request message: port  
<port number>, message code <message code>
```

Probable Cause

Indicates that the system is running low on resources when receiving an authentication request.

Recommended Action

Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

AUTH-1014

Message

```
<timestamp>, [AUTH-1014], <sequence-number>,, ERROR, <system-name>,  
Invalid port value to <operation>: port <port number>
```

Probable Cause

Indicates an internal problem with the Secure Fabric OS.

Recommended Action

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

AUTH-1017

Message

```
<timestamp>, [AUTH-1017], <sequence-number>,, ERROR, <system-name>,  
Invalid value to start authentication request: port <port number>,  
opcode <operation code>
```

Probable Cause

Indicates an internal problem with the Secure Fabric OS.

Recommended Action

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

AUTH-1018

Message

```
<timestamp>, [AUTH-1018], <sequence-number>,, ERROR, <system-name>,  
Invalid value to check protocol type: port <port number>
```

Probable Cause

Indicates an internal problem with the Secure Fabric OS.

Recommended Action

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

AUTH-1020

Message

```
<timestamp>, [AUTH-1020], <sequence-number>,, WARNING,  
<system-name>, Failed to create timer for authentication: port  
<port number>
```

Probable Cause

Indicates that an authentication message timer was not created.

Recommended Action

This is transient condition.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

AUTH-1022

Message

```
<timestamp>, [AUTH-1022], <sequence-number>,, ERROR, <system-name>,  
Failed to extract <data type> from <message> payload: port <port  
number>.
```

Probable Cause

Indicates the authentication process failed to extract a particular value from the receiving payload.

Recommended Action

Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

AUTH-1023

Message

```
<timestamp>, [AUTH-1023], <sequence-number>,, ERROR, <system-name>,  
Failed to <operation type> during <authentication phase>: port  
<port number>.
```

Probable Cause

Indicates an authentication operation failed for a certain authentication phase.

Operation type varies depending on authentication type:

- Some operations for SLAP: certificate retrieve, certificate verification signature verification, or nonce signing.
- Some operations for FCAP: certificate retrieve, certificate verification, signature verification, or nonce signing.
- Some operations for DH-CHAP: response calculation, challenge generation, or secret retrieve.

The *authentication phase* specifies which phase of a particular authentication protocol failed.

A nonce is a single-use, usually random value used in authentication protocols to prevent replay attacks.

Recommended Action

The error might indicate that an invalid entity tried to connect to the switch. Check the connection port for possible unauthorized access attack.

It might indicate that the PKI object for SLAP or FCAP or secret value for DH-CHAP on the local entity is not set up properly. Reinstall all PKI objects or reset the secret value for DH-CHAP properly.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

AUTH-1025

Message

```
<timestamp>, [AUTH-1025], <sequence-number>,, ERROR, <system-name>,  
Failed to get <data type> during <authentication phase>: port <port  
number>
```

Probable Cause

Indicates the authentication process failed to get expected information during the specified authentication phase.

Recommended Action

Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

AUTH-1027

Message

```
<timestamp>, [AUTH-1027], <sequence-number>,, ERROR, <system-name>,  
Failed to select <authentication value> during <authentication  
phase>: value <value> port <port number>.
```

Probable Cause

Indicates that the authentication process failed to select an authentication value (that is, DH Group, hash value, or protocol type) from a receiving payload for a particular authentication phase. This indicates that the local switch does not support the specified authentication value.

Recommended Action

Check the authentication configuration and reset the supported value if needed using the **authUtil** command.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

AUTH-1028

Message

```
<timestamp>, [AUTH-1028], <sequence-number>,, ERROR, <system-name>,  
Failed to allocate <data type> for <operation phase>: port <port  
number>
```

Probable Cause

Indicates that the authentication process failed because the system is low on memory.

Data type is the payload or structure that failed to get memory.

Operation phase specifies which operation of a particular authentication phase failed.

Recommended Action

Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

AUTH-1029

Message

```
<timestamp>, [AUTH-1029], <sequence-number>,, ERROR, <system-name>,  
Failed to get <data type> for <message phase> message: port <port  
number>, retval <error code>
```

Probable Cause

Indicates that the authentication process failed to get a particular authentication value at certain phase.

Recommended Action

Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

AUTH-1030

Message

```
<timestamp>, [AUTH-1030], <sequence-number>,, ERROR, <system-name>,  
Invalid message code for <message phase> message: port <port  
number>
```

Probable Cause

Indicates the receiving payload does not have valid message code for a particular authentication phase.

Recommended Action

Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

AUTH-1031

Message

```
<timestamp>, [AUTH-1031], <sequence-number>,, ERROR, <system-name>,  
Failed to retrieve secret value: port <port number>
```

Probable Cause

Indicates that the secret value was not set properly for the authenticated entity.

Recommended Action

Reset the secret value by using **secAuthSecret** command.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

Severity

ERROR

AUTH-1032

Message

```
<timestamp>, [AUTH-1032], <sequence-number>,, ERROR, <system-name>,  
Failed to generate <data type> for <message payload> payload:  
length <data length>, error code <error code>, port <port number>
```

Probable Cause

Indicates that the authentication process failed to generate a particular data (that is, challenge, nonce, or response data) for an authentication payload. This usually relates to internal failure. A nonce is a single-use, usually random value used in authentication protocols to prevent replay attacks.

Recommended Action

Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

AUTH-1033

Message

```
<timestamp>, [AUTH-1033], <sequence-number>,, ERROR, <system-name>,  
Disable port <port number> due to unauthorized switch <switch WWN  
value>
```

Probable Cause

Indicates that an entity was not configured in the SCC policy and tried to connect to the port.

Recommended Action

Add the entity's WWN to the SCC policy and reinitialize authentication by using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

Severity

ERROR

AUTH-1034

Message

```
<timestamp>, [AUTH-1034], <sequence-number>,, ERROR, <system-name>,  
Failed to validate name <entity name> in <authentication message>:  
port <port number>
```

Probable Cause

Indicates that the entity name in the payload is not in the right format.

Recommended Action

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

AUTH-1035

Message

```
<timestamp>, [AUTH-1035], <sequence-number>,, ERROR, <system-name>,  
Invalid <data type> length in <message phase> message: length <data  
length>, port <port number>
```

Probable Cause

Indicates that a particular data field in the authentication message has an invalid length field. This error usually relates to internal failure.

Recommended Action

Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

AUTH-1036

Message

```
<timestamp>, [AUTH-1036], <sequence-number>,, ERROR, <system-name>,  
Invalid state <state value> for <authentication phase>: port <port  
number>
```

Probable Cause

Indicates that the switch received an unexpected authentication message.

Recommended Action

Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

AUTH-1037

Message

```
<timestamp>, [AUTH-1037], <sequence-number>,, ERROR, <system-name>,  
Failed to <operation type> response for <authentication message>:  
init_len <data length>, resp_len <data length>, port <port number>.
```

Probable Cause

Indicates that a DH-CHAP authentication operation failed on the specified port due to mismatched response values between two entities.

Recommended Action

The error might indicate that an invalid entity tried to connect to the switch. Check the connection port for a possible security attack.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

AUTH-1038

Message

```
<timestamp>, [AUTH-1038], <sequence-number>,, ERROR, <system-name>,  
Failed to retrieve certificate during <authentication phase>: port  
<port number>
```

Probable Cause

Indicates that the PKI certificate is not installed properly.

Recommended Action

Reinstall the PKI certificate, using the **pkiCreate** command.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

BL error messages

BL-1000

Message

```
<timestamp>, [BL-1000], <sequence-number>,, INFO, <system-name>,  
Initializing Ports...
```

Probable Cause

Indicates that the switch has started initializing the ports. This message occurs only on the SAN Switch 4/32.

Recommended Action

No action is required.

Severity

INFO

BL-1001

Message

```
<timestamp>, [BL-1001], <sequence-number>,, INFO, <system-name>,  
Port Initialization Completed
```

Probable Cause

Indicates that the switch has completed initializing the ports. This message occurs only on the SAN Switch 4/32.

Recommended Action

No action is required.

Severity

INFO

BL-1002

Message

```
<timestamp>, [BL-1002], <sequence-number>,, CRITICAL,  
<system-name>, Init Failed: DISABLED because internal ports were  
not ONLINE, <slot number> <List of internal ports not ONLINE>
```

Probable Cause

Indicates that the blade initiation failed because one or more of the internal ports was not online. The blade is faulted. This message occurs on only the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.

Recommended Action

Make sure that the blade is seated correctly. If the blade is seated correctly, reboot or power cycle the blade.

Run the **systemVerification** command to verify that the blade does not have hardware problems. Refer to the *HP StorageWorks Fabric OS 5.x command reference guide* for more information on this command.

Additional blade fault messages precede and follow this error, providing more information. See other error messages for recommended action.

If the message persists, replace the blade.

Severity

CRITICAL

BL-1003

Message

```
<timestamp>, [BL-1003], <sequence-number>,, CRITICAL,  
<system-name>, Faulting blade in slot <slot number>
```

Probable Cause

Indicates a faulty blade in the specified slot number. This message occurs on only the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.

Recommended Action

Make sure that the blade is seated correctly. If the blade is seated correctly, reboot or power cycle the blade.

Run the **systemVerification** command to verify that blade does not have hardware problems. Refer to the *HP StorageWorks Fabric OS 5.x command reference guide* for more information on this command.

If the message persists, replace the blade.

Severity

CRITICAL

BL-1004

Message

```
<timestamp>, [BL-1004], <sequence-number>,, CRITICAL,  
<system-name>, Suppressing blade fault in slot <slot number>
```

Probable Cause

Indicates that the specified blade experienced a failure but was not faulted due to a user setting. This message occurs on only the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.

Recommended Action

Reboot or power cycle the blade, using the **slotPowerOff** and **slotPowerOn** commands.

Run the **systemVerification** command to verify that the blade does not have hardware problems. Refer to the *HP StorageWorks Fabric OS 5.x command reference guide* for more information on this command.

If the message persists, replace the blade.

Severity

CRITICAL

BL-1006

Message

```
<timestamp>, [BL-1006], <sequence-number>,, INFO, <system-name>,  
Blade <slot number> NOT faulted. Peer blade <slot number>  
experienced abrupt failure.
```

Probable Cause

Indicates that the errors (mostly synchronization errors) on this blade are harmless. Probably, the standby CP blade connected to the active CP blade has experienced transitory problems. This message occurs only on the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.

Recommended Action

Verify that the standby CP is healthy. If the standby CP was removed or faulted by user intervention, no action is required.

Severity

INFO

BL-1007

Message

```
<timestamp>, [BL-1007], <sequence-number>,, WARNING, <system-name>,  
blade #<blade number>: blade state is inconsistent with EM.  
bl_cflags 0x<blade control flags>, slot_on <slot_on flag>, slot_off  
<slot_off flag>, faulty <faulty flag>, status <blade status>
```

Probable Cause

Indicates that a failover occurred while a blade was initializing on the previously active CP. This message occurs on only the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.

Recommended Action

No action is required. The blade is reinitialized. Because reinitializing a blade is a disruptive operation and can stop I/O traffic, you might have to stop and restart the traffic during this process.

Severity

WARNING

BL-1008

Message

```
<timestamp>, [BL-1008], <sequence-number>,, CRITICAL,  
<system-name>, Slot <slot number> control-plane failure. Expected  
value: 0x<value 1>, Actual: 0x<value 2>
```

Probable Cause

Possibly the blade has experienced a hardware failure or was removed without following the recommended removal procedure. This message occurs on only the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.

Recommended Action

Make sure that the blade is seated correctly.

If the blade is seated correctly, reboot or power cycle the blade.

Run the **systemVerification** command to verify that the blade does not have hardware problems. Refer to the *HP StorageWorks Fabric OS 5.x command reference guide* for more information on this command.

If the message persists, replace the blade.

Severity

CRITICAL

BL-1009

Message

```
<timestamp>, [BL-1009], <sequence-number>,, CRITICAL,  
<system-name>, Blade in slot <slot number> timed out initializing  
the chips.
```

Probable Cause

Indicates that the blade has failed to initialize the ASIC chips. This message occurs on only the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.

Recommended Action

Make sure that the blade is seated correctly.

If the blade is seated correctly, reboot or power cycle the blade.

Run the **systemVerification** command to verify that the blade does not have hardware problems. Refer to the *HP StorageWorks Fabric OS 5.x command reference guide* for more information on this command.

If the message persists, replace the blade.

Severity

CRITICAL

BL-1010

Message

```
<timestamp>, [BL-1010], <sequence-number>,, WARNING, <system-name>,  
Blade in slot <slot number> inconsistent with the hardware  
settings.
```

Probable Cause

Indicates that a failover occurred while some hardware changes were being made on the previously active CP (such as changing the domain ID). This message occurs on only the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.

Recommended Action

No action is required. This blade has been reinitialized. Because reinitializing a blade is a disruptive operation and can stop I/O traffic, you might have to stop and restart the traffic during this process.

Severity

WARNING

BL-1011

Message

```
<timestamp>, [BL-1011], <sequence-number>,, CRITICAL,  
<system-name>, Busy with emb-port int. for chip <chip number> in  
minis <minis number> on blade <slot number>, chip int. is disabled.  
interrupt status=0x<interrupt status>
```

Probable Cause

Indicates that too many interrupts in the embedded port caused the specified chip to be disabled. The probable cause is too many abnormal frames; the chip is disabled to prevent the CP from becoming too busy.

Recommended Action

Make sure to capture the console output during this process.

Check for a faulty cable, SFP, or device attached to the specified port.

Run the **systemVerification** command to verify that the blade or switch does not have hardware problems.

On a bladed switch, run the **slotPowerOff** and **slotPowerOn** commands.

On a nonbladed switch, reboot or power cycle the switch.

If the message persists, replace the blade or the (nonbladed) switch.

Severity

CRITICAL

BL-1012

Message

```
<timestamp>, [BL-1012], <sequence-number>,, ERROR, <system-name>,  
bport <port number> port int. is disabled. status=0x<interrupt  
status> Port <port number> will be re-enabled in 1 minute.
```

Probable Cause

Indicates that the port generated an excessive number of interrupts that might prove fatal to the switch operation. The port is disabled to prevent the CP from becoming too busy. The bport is the blade port; this number might not correspond to a user port number.

Recommended Action

Make sure to capture the console output during this process.

Check for a faulty cable, SFP, or device attached to the specified port.

On a bladed switch, run the **slotPowerOff** and **slotPowerOn** commands.

On a nonbladed switch, reboot or power cycle the switch.

If the message persists, replace the blade or the (nonbladed) switch.

Severity

ERROR

BL-1013

Message

```
<timestamp>, [BL-1013], <sequence-number>,, ERROR, <system-name>,  
bport <port number> port is faulted. status=0x<interrupt status>  
Port <port number> will be re-enabled in 1 minute.
```

Probable Cause

Indicates that the port generated an excessive number of interrupts that might prove fatal to the switch operation. The port is disabled to prevent the CP from becoming too busy. The bport is the blade port; this number might not correspond to a user port number.

Recommended Action

Make sure to capture the console output during this process.

Check for a faulty cable, SFP, or device attached to the specified port.

On a bladed switch, run the **slotPowerOff** and **slotPowerOn** commands.

On a nonbladed switch, reboot or power cycle the switch.

If the message persists, replace the blade.

Severity

ERROR

BL-1014

Message

```
<timestamp>, [BL-1014], <sequence-number>,, ERROR, <system-name>,  
bport <port number> port int. is disabled. status=0x<interrupt  
status>
```

Probable Cause

Indicates that the port generated an excessive number of interrupts that might prove fatal to the switch operation. The port is disabled to prevent the CP from becoming too busy. The bport is the blade port; this number might not correspond to a user port number.

Recommended Action

Make sure to capture the console output during this process.

On a bladed switch, run the **slotPowerOff** and **slotPowerOn** commands.

On a nonbladed switch, **reboot** the switch.

Run the **systemVerification** command to determine if there is a hardware error.

If there is a hardware error, if the **slotPowerOff** or **slotPowerOn** fails on the bladed switch or if errors are encountered again:

- On the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, replace the blade FRU.
- On the SAN Switch 2/32, replace the motherboard FRU.
- On the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, or SAN Switch 4/32, replace the switch.

Severity

ERROR

BL-1015

Message

```
<timestamp>, [BL-1015], <sequence-number>,, ERROR, <system-name>,  
bport <port number> port is faulted. status=0x<interrupt status>
```

Probable Cause

Indicates that the port generated an excessive number of interrupts that might prove fatal to the switch operation. The port is disabled to prevent the CP from becoming too busy. The bport is the blade port; this number might not correspond to a user port number.

Recommended Action

Make sure to capture the console output during this process.

On a bladed switch, run the **slotPowerOff** and **slotPowerOn** commands.

On a nonbladed switch, **reboot** the switch.

Run the **systemVerification** command to determine if there is a hardware error.

If there is a hardware error, if the **slotPowerOff** or **slotPowerOn** fails on the bladed switch or if errors are encountered again:

- On the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, replace the blade FRU.
- On the SAN Switch 2/32, replace the motherboard FRU.

- On the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, or SAN Switch 4/32, replace the switch.

Severity

ERROR

BL-1016

Message

```
<timestamp>, [BL-1016], <sequence-number>,, CRITICAL,  
<system-name>, Blade port <port number> in slot <slot number>  
failed to enable.
```

Probable Cause

Indicates that the specified blade port has failed to get enabled.

Recommended Action

Make sure that the blade is seated correctly.

If the blade is seated correctly, reboot or power cycle the blade.

Run the **systemVerification** command to verify that the blade does not have hardware problems. Refer to the *HP StorageWorks Fabric OS 5.x command reference guide* for more information on this command.

If the message persists, replace the blade.

Severity

CRITICAL

BL-1017

Message

```
<timestamp>, [BL-1017], <sequence-number>,, INFO, <system-name>,  
Slot <port number> initializing...
```

Probable Cause

Indicates that the slot has started initializing ports.

Recommended Action

No action is required.

Severity

INFO

BL-1018

Message

```
<timestamp>, [BL-1018], <sequence-number>,, INFO, <system-name>,  
Slot <port number> Initialization Completed
```

Probable Cause

Indicates that the slot has completed initializing the ports.

Recommended Action

No action is required.

Severity

INFO

BLL Error Messages

BLL-1000

Message

```
<timestamp>, [BLL-1000], <sequence-number>,, CRITICAL,  
<system-name>, ASIC driver detected Slot <slot number> port <port  
number> as faulty (reason: <reason>)
```

Probable Cause

Indicates that a blade regulation problem was reported on the specified *slot number*. The blade is faulted. This message occurs on only the Core Switch 2/64 and SAN Director 2/128.

The reason codes are as follows:

- 1 = Available buffer overflow
- 2 = Backend port buffer timeout
- 3 = Backend port got shut down
- 4 = Embedded port buffer timeout
- 5 = Excessive busy mini buffer
- 6 = Excessive RCC VC on E_Port
- 7 = Excessive RCC VC on FL_Port
- 8 = Fail detection buffer tag error
- 9 = Fail detection TX parity error
- 10 = EPI CMEM interrupt error
- 11 = CMI interrupt error
- 12 = Interrupt overrun
- 13 = FDET interrupt
- 14 = Interrupt suspended
- 15 = Filter LISTD error
- 16 = Unknown filter LIST error
- 17 = Wait for LPC open state
- 18 = Wait for Old port state
- 19 = Wait for Open init state
- 20 = TX parity error
- 21 = RAM parity error
- 22 = BISR or RAMINIT error

Recommended Action

Make sure that the blade is seated correctly.

If the blade is seated correctly, reboot or power cycle the blade.

Run the **systemVerification** command to verify that the blade does not have hardware problems. Refer to the *HP StorageWorks Fabric OS 5.x command reference guide* for more information on this command.

If the message persists, replace the blade.

Severity

CRITICAL

CDR error messages

CDR-1001

Message

```
<timestamp>, [CDR-1001], <sequence-number>,, WARNING,  
<system-name>, Port <port number> port fault. Please change the SFP  
or check cable
```

Probable Cause

Indicates either a deteriorated SFP, an incompatible SFP pair, or a faulty cable between peer ports.

Recommended Action

Verify that you are using compatible SFPs on the peer ports.

Verify that the SFPs have not deteriorated and that the Fibre Channel cable is not faulty. Replace the SFPs or cable if necessary.

Severity

WARNING

CER-1001 error messages

CER-1001

Message

```
<timestamp>, [CER-1001], <sequence-number>,, ERROR, <system-name>,  
HA Sync broken, since standby Advanced Performance Tuning module  
does not support FICON Management Server (FMS).
```

Probable Cause

Indicates that the HA synchronization between the active and standby CPs is broken because there is downlevel firmware loaded on the standby CP. The standby CP does not support the Advanced Performance Tuning module when FICON Management Server is enabled.

Recommended Action

Run the **firmwareDownload** command to upgrade the firmware on the standby CP.

You can also disable FMS on the active CP.

Severity

ERROR

CONF error messages

CONF-1000

Message

```
<timestamp>, [CONF-1000], <sequence-number>,, WARNING,  
<system-name>, configDownload completed successfully but Zoning and  
Security parts were ignored
```

Probable Cause

Indicates that the user with the switchadmin role does not have permission to update the Zoning and Security configurations, so the Zoning and Security configurations are skipped while downloading the configuration file.

Recommended Action

No action is required. You must login as admin to update the Zoning and Security configurations using the **configDownload** command.

Severity

WARNING

EM error messages

EM-1001

Message

```
<timestamp>, [EM-1001], <sequence-number>,, CRITICAL,  
<system-name>, <FRU Id> is over heating: Shutting down
```

Probable Cause

Indicates that a field replaceable unit (FRU) is shutting down due to overheating. This is typically due to a faulty fan but can also be caused by the switch environment.

Recommended Action

Verify that the location temperature is within the operational range of the switch. Refer to the hardware reference manual for the environmental temperature range of your switch.

Run the **fanShow** command to verify that all fans are running at normal speeds. If any fans are missing or are not performing at high enough speed, they should be replaced. Healthy fan speeds are as follows:

- 4/256 SAN Director fans run at approximately 2500 RPM.
- SAN Director 2/128 fans run at approximately 2500 RPM.
- Core Switch 2/64 fans run at approximately 2500 RPM.
- SAN Switch 4/32 fans run at approximately 6000 RPM.
- SAN Switch 2/32 fans run at approximately 3500 RPM.
- SAN Switch 2/16V fans run at approximately 9000 RPM.
- SAN Switch 2/8V fans run at approximately 5500 RPM.
- 4/8 SAN Switch, 4/16 SAN Switch has 4 fans. The 4/8 SAN Switch, 4/16 SAN Switch fans do not have RPM sensors, so cannot display fan speed.

The SAN Switch 2/8V has three fans, and the SAN Switch 2/16V has four fans. Values for the individual fans might display in this message, but these parts cannot be replaced: the entire switch is a FRU.

Severity

CRITICAL

EM-1002

Message

```
<timestamp>, [EM-1002], <sequence-number>,, CRITICAL,  
<system-name>, System fan(s) status <fan fru>
```

Probable Cause

Indicates that a nonbladed system has overheated and is going to shut down. Before doing so, all fan speeds are dumped to the console.

Recommended Action

Verify that the location temperature is within the operational range of the switch. Refer to the hardware reference manual for the environmental temperature range of your switch.

Run the **fanShow** command to verify that all fans are running at normal speeds. If any fans are missing or are not performing at high enough speed, they should be replaced. Healthy fan speeds are as follows:

- 4/256 SAN Director fans run at approximately 2500 RPM.
- SAN Director 2/128 fans run at approximately 2500 RPM.
- Core Switch 2/64 fans run at approximately 2500 RPM.
- SAN Switch 4/32 fans run at approximately 6000 RPM.
- SAN Switch 2/32 fans run at approximately 3500 RPM.
- SAN Switch 2/16V fans run at approximately 9000 RPM.
- SAN Switch 2/8V fans run at approximately 5500 RPM.
- 4/8 SAN Switch, 4/16 SAN Switch has 4 fans. The 4/8 SAN Switch, 4/16 SAN Switch fans do not have RPM sensors, so cannot display fan speed.

The SAN Switch 2/8V has three fans, and the SAN Switch 2/16V has four fans. Values for the individual fans might display in this message, but these parts cannot be replaced: the entire switch is a FRU.

Severity

CRITICAL

EM-1003

Message

```
<timestamp>, [EM-1003], <sequence-number>,, CRITICAL,  
<system-name>, <FRU Id> has unknown hardware identifier: FRU  
faulted.
```

Probable Cause

Indicates that a fan FRU header could not be read or is not valid. The FRU is faulted.

Recommended Action

On Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, try reseating the specified FRU.

Reboot or power cycle the switch.

Run the **systemVerification** command to verify that the switch does not have hardware problems. Refer to the *HP StorageWorks Fabric OS 5.x command reference guide* for more information on this command.

On the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, replace the specified FRU.

For the SAN Switch 2/32, replace the motherboard FRU.

For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, and SAN Switch 4/32 you must replace the switch.

Severity

CRITICAL

EM-1004

Message

```
<timestamp>, [EM-1004], <sequence-number>,, CRITICAL,  
<system-name>, <FRU Id> failed to power on
```

Probable Cause

Indicates that a FRU failed to power on and is not being used. The type of FRU is specified in the message.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- Switch for fixed port count switches.
- *Slot 1* through *Slot 10* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.
- *PS 1* through *PS 4* (power supplies) for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, or *PS 1* through *PS 2* for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *Fan 1* through *Fan 3* for the Core Switch 2/64, SAN Director 2/128, 4/256 SAN Director, and SAN Switch 4/32 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *WWN 1* or *WWN 2* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.

The does not have any fans, power supplies or WWN cards.

The 4/8 SAN Switch, 4/16 SAN Switch has 4 fans and 1 power supply, but these parts cannot be replaced: the entire switch is a FRU.

Recommended Action

Try reseating the FRU. If the message persists, replace the FRU.

Severity

CRITICAL

EM-1005

Message

```
<timestamp>, [EM-1005], <sequence-number>,, CRITICAL,  
<system-name>, <FRU Id> has faulted. Sensor(s) above maximum limits
```

Probable Cause

Indicates that a blade in the specified slot or the switch (for nonbladed switches) is being shut down for environmental reasons; its temperature or voltage is out of range.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- Switch for fixed port count switches.
- *Slot 1* through *Slot 10* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.

Recommended Action

Check the environment and make sure the room temperature is within the operational range of the switch. Use the **fanShow** command to verify fans are operating properly. Make sure there are no blockages of the airflow around the chassis. If the temperature problem is isolated to the blade itself, replace the blade.

Voltage problems on a blade are likely a hardware problem on the blade itself; replace the blade.

Severity

CRITICAL

EM-1006

Message

```
<timestamp>, [EM-1006], <sequence-number>,, CRITICAL,  
<system-name>, <FRU Id> has faulted. Sensor(s) below minimum limits
```

Probable Cause

Indicates that the sensors show the voltage is below minimum limits. The switch or specified blade is being shut down for environmental reasons; the voltage is too low.

Recommended Action

If this problem occurs on a blade, it usually indicates a hardware problem on the blade; replace the blade.

If this problem occurs on a switch, it usually indicates a hardware problem on the main board; replace the switch.

Severity

CRITICAL

EM-1007

Message

```
<timestamp>, [EM-1007], <sequence-number>,, CRITICAL,  
<system-name>, <FRU Id> is being reset. Sensor(s) has exceeded max  
limits
```

Probable Cause

Indicates that the voltage on a switch has exceeded environmental limits. A reset is sent to the faulty slot or the switch for nonbladed switches.

Recommended Action

There is most likely a voltage hardware problem on the blade or motherboard of the switch.

For the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, replace the blade FRU.

For the SAN Switch 2/32 and SAN Switch 4/32, replace the motherboard FRU.

For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, and SAN Switch 2/16V you must replace the switch.

Severity

CRITICAL

EM-1008

Message

```
<timestamp>, [EM-1008], <sequence-number>,, CRITICAL,  
<system-name>, Unit in <FRU Id> faulted, incompatible with chassis  
option <Chassis configuration option>
```

Probable Cause

Indicates that a blade inserted in the specified slot is not compatible with the switch **chassisConfig** option. The blade is faulted. This message occurs only on the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.

Recommended Action

Replace the blade. Make sure the replacement blade is compatible with your CP type and **chassisConfig** setting.

Severity

CRITICAL

EM-1009

Message

```
<timestamp>, [EM-1009], <sequence-number>,, CRITICAL,  
<system-name>, <FRU Id> powered down unexpectedly
```

Probable Cause

Indicates that the environmental monitor (EM) received an unexpected power-down notification from the specified FRU. This might indicate a hardware malfunction in the FRU. This message occurs only on the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- Switch for fixed port count switches.
- *Slot 1* through *Slot 10* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.
- *PS 1* through *PS 4* (power supplies) for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, or *PS 1* through *PS 2* for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *Fan 1* through *Fan 3* for the Core Switch 2/64, SAN Director 2/128, 4/256 SAN Director, and SAN Switch 4/32 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *WWN 1* or *WWN 2* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

Recommended Action

Try reseating the FRU. If the message persists, replace the FRU.

Severity

CRITICAL

EM-1010

Message

```
<timestamp>, [EM-1010], <sequence-number>,, CRITICAL,  
<system-name>, Received unexpected power down for <FRU Id> But <FRU  
Id> still has power
```

Probable Cause

Indicates that the environmental monitor received an unexpected power-down notification from the specified FRU. However, the specified FRU still appears to be powered up after four seconds. This message occurs only on the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.

Recommended Action

Try reseating the blade. If this fails to correct the error, replace the blade.

Severity

CRITICAL

EM-1011

Message

```
<timestamp>, [EM-1011], <sequence-number>,, CRITICAL,  
<system-name>, Received unexpected power down for <FRU Id>, but  
cannot determine if it has power
```

Probable Cause

Indicates that the environmental monitor (EM) received an unexpected power-down notification from the FRU specified; however, after four seconds it cannot be determined if it has powered down or not. This message occurs only on the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.

Recommended Action

Try reseating the blade. If this fails to correct the error, replace the blade.

Severity

CRITICAL

EM-1012

Message

```
<timestamp>, [EM-1012], <sequence-number>,, CRITICAL,  
<system-name>, <FRU Id> failed <state> state transition, fru  
faulted
```

Probable Cause

Indicates that a switch blade failed to transition from one state to another. It is faulted. The specific failed target state is displayed in the message. There are serious internal Fabric OS configuration or hardware problems on the switch.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- Switch for fixed port count switches.
- *Slot 1* through *Slot 10* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.

Recommended Action

On Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, try reseating the indicated FRU.

If the message persists, reboot or power cycle the switch.

Run the **systemVerification** command to verify that the switch does not have hardware problems. Refer to the *HP StorageWorks Fabric OS 5.x command reference guide* for more information on this command.

If the message persists, replace the FRU.

Severity

CRITICAL

EM-1013

Message

```
<timestamp>, [EM-1013], <sequence-number>,, ERROR, <system-name>,  
Failed to update FRU information for <FRU Id>
```

Probable Cause

Indicates that the environmental monitor was unable to update the time alive or OEM data in the memory on a FRU.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- Switch for fixed port count switches.
- *Slot 1* through *Slot 10* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.
- *PS 1* through *PS 4* (power supplies) for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, or *PS 1* through *PS 2* for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *Fan 1* through *Fan 3* for the Core Switch 2/64, SAN Director 2/128, 4/256 SAN Director, and SAN Switch 4/32 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *WWN 1* or *WWN 2* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.

The does not have any fans, power supplies or WWN cards.

The 4/8 SAN Switch, 4/16 SAN Switch has 4 fans and 1 power supply, but these parts cannot be replaced: the entire switch is a FRU.

Recommended Action

If the **fruInfoSet** command was being run, try the command again; otherwise, the update is automatically reattempted. If it continues to fail, try reseating the FRU.

If the message persists, replace the FRU.

Severity

ERROR

EM-1014

Message

```
<timestamp>, [EM-1014], <sequence-number>,, ERROR, <system-name>,  
Unable to read sensor on <FRU Id> (<Return code>)
```

Probable Cause

Indicates that the environmental monitor was unable to access the sensors on the specified FRU.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- Switch for fixed port count switches.
- *Slot 1* through *Slot 10* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.
- *PS 1* through *PS 4* (power supplies) for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, or *PS 1* through *PS 2* for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *Fan 1* through *Fan 3* for the Core Switch 2/64, SAN Director 2/128, 4/256 SAN Director, and SAN Switch 4/32 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *WWN 1* or *WWN 2* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.

The does not have any fans, power supplies or WWN cards.

The 4/8 SAN Switch, 4/16 SAN Switch has 4 fans and 1 power supply, but these parts cannot be replaced: the entire switch is a FRU.

Recommended Action

Try reseating the FRU. If the message persists, replace the FRU.

Severity

ERROR

EM-1015

Message

```
<timestamp>, [EM-1015], <sequence-number>,, WARNING, <system-name>,  
Warm recovery failed (<Return code>)
```


Probable Cause

Indicates that a problem was discovered when performing consistency checks during a warm boot.

Recommended Action

A **reboot** or power cycle is required to clear the situation.

Severity

WARNING

EM-1016

Message

```
<timestamp>, [EM-1016], <sequence-number>,, WARNING, <system-name>,  
Cold recovery failed (<Return code>)
```

Probable Cause

Indicates that consistency checks during a cold boot discovered a problem.

Recommended Action

Monitor the switch.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

EM-1017

Message

```
<timestamp>, [EM-1017], <sequence-number>,, WARNING, <system-name>,  
Uncommitted WWN change detected. Cold reboot required.
```

Probable Cause

Indicates that a user did not commit a changed WWN value prior executing a **reboot**, power cycle, or **firmwareDownload** operation.

Recommended Action

Change and commit the new WWN value.

Severity

WARNING

EM-1018

Message

```
<timestamp>, [EM-1018], <sequence-number>,, CRITICAL,  
<system-name>, CP blade in slot <Slot number> failed to retrieve  
current chassis type <Detailed fault descriptor>
```

Probable Cause

Indicates that there was a failure to read chassis type from the system.

Recommended Action

Verify that the CP blade is operational and properly seated in the slot.

Severity

CRITICAL

EM-1019

Message

```
<timestamp>, [EM-1019], <sequence-number>,, WARNING, <system-name>,  
Current chassis configuration option <Chassis config option  
currently in effect> is not compatible with standby firmware  
version (Pre 4.4), cannot allow HA Sync
```

Probable Cause

Indicates that the current chassis config option is not supported by the firmware on the standby CP. This is true even if the standby comes up and appears to be operational. HA synchronization of the CPs will not be allowed.

Recommended Action

Use the **chassisConfig** command to change the chassis config option to 1, or upgrade the firmware on the standby CP to match the firmware on the active CP.

Severity

WARNING

EM-1028

Message

```
<timestamp>, [EM-1028], <sequence-number>,, CRITICAL,  
<system-name>, HIL Error: <function> failed to access FRU: <FRU Id>  
(rc=<return code>).
```

Probable Cause

Indicates that problems were encountered when the software attempted to write to the memory of the FRU specified in the error message. The return code is for internal use only. This is a serious FRU hardware problem.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- Switch for fixed port count switches.
- *Slot 1* through *Slot 10* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.
- *PS 1* through *PS 4* (power supplies) for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, or *PS 1* through *PS 2* for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *Fan 1* through *Fan 3* for the Core Switch 2/64, SAN Director 2/128, 4/256 SAN Director, and SAN Switch 4/32 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.

- *WWN 1* or *WWN 2* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.

The does not have any fans, power supplies or WWN cards.

The 4/8 SAN Switch, 4/16 SAN Switch has 4 fans and 1 power supply, but these parts cannot be replaced: the entire switch is a FRU.

Recommended Action

Try reseating the FRU. If the message persists, replace the FRU.

Severity

CRITICAL

EM-1029

Message

```
<timestamp>, [EM-1029], <sequence-number>,, ERROR, <system-name>,  
<FRU Id> I2C access problems (<error code>): state <current state>
```

Probable Cause

Indicates that the I2C bus had problems and a timeout occurred.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- Switch for fixed port count switches.
- *Slot 1* through *Slot 10* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.
- *PS 1* through *PS 4* (power supplies) for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, or *PS 1* through *PS 2* for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *Fan 1* through *Fan 3* for the Core Switch 2/64, SAN Director 2/128, 4/256 SAN Director, and SAN Switch 4/32 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *WWN 1* or *WWN 2* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.

The does not have any fans, power supplies or WWN cards.

The 4/8 SAN Switch, 4/16 SAN Switch has 4 fans and 1 power supply, but these parts cannot be replaced: the entire switch is a FRU.

Recommended Action

This is often a transient error.

Watch for the EM-1048 message, which indicates that the problem has been resolved.

If the error persists, check for loose or dirty connections. Remove all dust and debris prior to reseating the FRU. If it continues to fail, replace the FRU.

Severity

ERROR

EM-1031

Message

```
<timestamp>, [EM-1031], <sequence-number>,, ERROR, <system-name>,  
<FRU Id> ejector not closed
```

Probable Cause

Indicates that the environmental monitor (EM) has found a switch blade that is inserted, but at least one ejector switch is not latched. The blade in the specified slot is treated as not inserted. This message occurs only on the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.

Recommended Action

Close the ejector switch if the FRU is intended for use.

Severity

ERROR

EM-1033

Message

```
<timestamp>, [EM-1033], <sequence-number>,, ERROR, <system-name>,  
CP in <FRU Id> set to faulty because CP ERROR asserted
```

Probable Cause

Indicates that the standby CP has been detected as faulty. The High Availability feature will not be available. This message occurs every time the other CP reboots, even as part of a clean warm failover. In most situations, this message is followed by the EM-1047 message, and no action is required for the CP; however, you might want to find out why the failover occurred. This message occurs only on the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.

Recommended Action

If the standby CP was just rebooted, wait for the error to clear (run **slotShow** to determine if it has cleared). Watch for the EM-1047 message to verify this error cleared.

If the standby CP continues to be faulty or if it was not intentionally rebooted, check the error logs on the other CP (using the **errDump** command) to determine the cause of the error state.

Try reseating the FRU. If the message persists, replace the FRU.

Severity

ERROR

EM-1034

Message

```
<timestamp>, [EM-1034], <sequence-number>,, ERROR, <system-name>,  
<FRU Id> set to faulty, rc=<return code>
```

Probable Cause

Indicates that the specified FRU has been marked as faulty for the specified reason.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- Switch for fixed port count switches.
- *Slot 1* through *Slot 10* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.
- *PS 1* through *PS 4* (power supplies) for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, or *PS 1* through *PS 2* for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *Fan 1* through *Fan 3* for the Core Switch 2/64, SAN Director 2/128, and SAN Switch 4/32 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *WWN 1* or *WWN 2* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.

The does not have any fans, power supplies or WWN cards.

The 4/8 SAN Switch, 4/16 SAN Switch has 4 fans and 1 power supply, but these parts cannot be replaced: the entire switch is a FRU.

Recommended Action

Try reseating the FRU.

Run the **systemVerification** command to verify that the switch does not have hardware problems. Refer to the *HP StorageWorks Fabric OS 5.x command reference guide* for more information on this command.

If the message persists, replace the FRU.

Severity

ERROR

EM-1035

Message

```
<timestamp>, [EM-1035], <sequence-number>,, ERROR, <system-name>, 2  
circuit paired PS's are faulty, please check the <switch side> AC  
main switch/circuit to see if it has power.
```

Probable Cause

Indicates that both Power Supplies associated with one of the two main circuits are present but faulty, that the circuit's switch has been turned off, or the AC power source has been interrupted for that circuit.

The *<switch side>* value is either *left* or *right* designating which circuit switch, facing the cable side of the chassis is possibly disabled. The switch side value indicates:

- *left*: controls the odd numbered power supply units.
- *right*: controls the even numbered power supply units.

This message only occurs on the Core Switch 2/64, SAN Director 2/128, or 4/256 SAN Director.

Recommended Action

Check that the identified AC circuit switch is turned on, that the power cord is properly attached and undamaged, and that the power source is operating properly.

Severity

ERROR

EM-1036

Message

```
<timestamp>, [EM-1036], <sequence-number>,, WARNING, <system-name>,  
<FRU Id> is not accessible.
```

Probable Cause

Indicates that the specified FRU does not seem to be present on the switch.

If the FRU is a WWN card, then default WWN and IP addresses are used for the switch.

Recommended Action

Reseat the FRU card.

If the message persists, reboot or power cycle the switch.

Run the **systemVerification** command to verify that the switch does not have hardware problems. Refer to the *HP StorageWorks Fabric OS 5.x command reference guide* for more information on this command.

If the message persists, replace the FRU.

Severity

WARNING

EM-1041

Message

```
<timestamp>, [EM-1041], <sequence-number>,, WARNING, <system-name>,  
Sensor values for <FRU Id>: <Sensor Value> <Sensor Value> <Sensor  
Value> <Sensor Value> <Sensor Value> <Sensor Value> <Sensor Value>
```

Probable Cause

Indicates that sensors detected a warning condition. All significant sensors for the FRU are displayed; each contains a header.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- Switch for fixed port count switches.
- *Slot 1* through *Slot 10* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.
- *PS 1* through *PS 4* (power supplies) for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, or *PS 1* through *PS 2* for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *Fan 1* through *Fan 3* for the Core Switch 2/64, SAN Director 2/128, and SAN Switch 4/32 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.

- WWN 1 or WWN 2 for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.

The does not have any fans, power supplies or WWN cards.

The 4/8 SAN Switch, 4/16 SAN Switch has 4 fans and 1 power supply, but these parts cannot be replaced: the entire switch is a FRU. The 4/8 SAN Switch, 4/16 SAN Switch fans do not have RPM sensors, so cannot display fan speed.

This message can display:

- voltages in volts
- temperature in Celsius
- fan speeds in RPM

Recommended Action

If the message is isolated, monitor the error messages on the switch. If the message is associated with other messages, follow the recommended action for those messages.

Severity

WARNING

EM-1042

Message

```
<timestamp>, [EM-1042], <sequence-number>,, WARNING, <system-name>,
Important FRU header data for <FRU Id> is not valid).
```

Probable Cause

Indicates that the indicated FRU has an incorrect number of sensors in its FRU header-derived information. This could mean that the FRU header was corrupted or read incorrectly or corrupted in the object database, which contains information about all FRUs.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- Switch for fixed port count switches.
- *Slot 1* through *Slot 10* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.
- *PS 1* through *PS 4* (power supplies) for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, or *PS 1* through *PS 2* for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *Fan 1* through *Fan 3* for the Core Switch 2/64, SAN Director 2/128, and SAN Switch 4/32 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- WWN 1 or WWN 2 for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.

The does not have any fans, power supplies or WWN cards.

The 4/8 SAN Switch, 4/16 SAN Switch has 4 fans and 1 power supply, but these parts cannot be replaced: the entire switch is a FRU.

Recommended Action

Try reseating the FRU. If the message persists, replace the FRU.

Severity

WARNING

EM-1043

Message

```
<timestamp>, [EM-1043], <sequence-number>,, WARNING, <system-name>,  
Can't power <FRU Id> <state (on or off)>.
```

Probable Cause

Indicates that the specified FRU cannot be powered on or off.

Recommended Action

The specified FRU is not responding to commands and should be replaced.

Severity

WARNING

EM-1044

Message

```
<timestamp>, [EM-1044], <sequence-number>,, WARNING, <system-name>,  
Can't power on <FRU Id>, its logical switch is shut down
```

Probable Cause

Indicates that the specified FRU cannot be powered on because the associated logical switch is shut down. This message only occurs on the Core Switch 2/64, and SAN Director 2/128.

Recommended Action

Run the **switchStart** command on the associated logical switch.

Severity

WARNING

EM-1045

Message

```
<timestamp>, [EM-1045], <sequence-number>,, WARNING, <system-name>, <FRU Id> is  
being powered <new state>
```

Probable Cause

Indicates that an automatic power adjustment is being made because of the (predicted) failure of a power supply or the insertion or removal of a port blade. If new_state is On, a port blade is being powered on because more power is available (either a power supply was inserted or a port blade was removed or powered down). If new_state is Off, a port blade has been powered down because a power supply has

been faulted, because it is indicating a predicted failure. If new_state is Down (not enough power), a newly inserted port blade was not powered on because there was not enough power available.

Recommended Action

The Core Switch 2/64 requires two power supplies for a fully populated chassis; however, you should always operate the system with four operating power supplies for redundancy.

The SAN Director 2/128 requires only a single power supply for a fully populated chassis; however, you should always operate the system with at least two power supplies for redundancy.

Severity

WARNING

EM-1046

Message

```
<timestamp>, [EM-1046], <sequence-number>,, WARNING, <system-name>, Sysctrl reports  
error status for blade ID <id value> for the blade in slot <slot number>
```

Probable Cause

Indicates that the system controller encountered a blade with an unknown ID in the slot specified. This message occurs only on the Core Switch 2/64 and SAN Director 2/128.

Recommended Action

The blade ID listed is not compatible with the **chassisConfig** option in effect. Use the **chassisConfig** command to see a list of compatible blade ID's for each option.

If the blade ID listed is not correct, then the FRU header for the blade is corrupted and the blade must be replaced. For the Core Switch 2/64, the blade ID should be 1 for a CP blade and 2 for a port blade. For the SAN Director 2/128, the blade ID should be 5 for a CP blade and 4 for a port blade. For the 4/256 SAN Director, the blade ID should be 16 for a CP blade and 17 or 18 for a port blade.

Severity

WARNING

EM-1047

Message

```
<timestamp>, [EM-1047], <sequence-number>,, INFO, <system-name>, CP  
in slot <slot number> not faulty, CP ERROR deasserted
```

Probable Cause

Indicates that the CP is no longer faulted. This message usually follows EM-1033. The new standby CP is in the process of rebooting and has turned off the CP_ERR signal. This message occurs only on the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.

Recommended Action

No action is required.

Severity

INFO

EM-1048

Message

```
<timestamp>, [EM-1048], <sequence-number>,, INFO, <system-name>, <FRU Id> I2C access  
recovered: state <current state>
```

Probable Cause

Indicates that the I2C bus problems have been resolved and I2C access to the FRU has become available again.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- Switch for fixed port count switches.
- *Slot 1* through *Slot 10* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.
- *PS 1* through *PS 4* (power supplies) for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, or *PS 1* through *PS 2* for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *Fan 1* through *Fan 3* for the Core Switch 2/64, SAN Director 2/128, and SAN Switch 4/32 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *WWN 1* or *WWN 2* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.

The does not have any fans, power supplies or WWN cards.

The 4/8 SAN Switch, 4/16 SAN Switch has 4 fans and 1 power supply, but these parts cannot be replaced: the entire switch is a FRU.

Recommended Action

The EM-1029 error can be a transitory error; if the problem resolves, the EM-1048 message is displayed.

Severity

INFO

EM-1049

Message

```
<timestamp>, [EM-1049], <sequence-number>,, INFO, <system-name>,  
FRU <FRU Id> insertion detected.
```

Probable Cause

Indicates that a FRU of the type and location specified by the FRU ID was detected as having been inserted into the chassis.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- Switch for fixed port count switches.
- *Slot 1* through *Slot 10* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.

- *PS 1* through *PS 4* (power supplies) for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, or *PS 1* through *PS 2* for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *Fan 1* through *Fan 3* for the Core Switch 2/64, SAN Director 2/128, and SAN Switch 4/32 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *WWN 1* or *WWN 2* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.

The does not have any fans, power supplies or WWN cards.

The 4/8 SAN Switch, 4/16 SAN Switch has 4 fans and 1 power supply, but these parts cannot be replaced: the entire switch is a FRU.

Recommended Action

No action is required.

Severity

INFO

EM-1050

Message

```
<timestamp>, [EM-1050], <sequence-number>,, INFO, <system-name>,  
FRU <FRU Id> removal detected.
```

Probable Cause

Indicates that a FRU of the specified type and location was removed from the chassis.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- Switch for fixed port count switches.
- *Slot 1* through *Slot 10* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.
- *PS 1* through *PS 4* (power supplies) for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, or *PS 1* through *PS 2* for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *Fan 1* through *Fan 3* for the Core Switch 2/64, SAN Director 2/128, and SAN Switch 4/32 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *WWN 1* or *WWN 2* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. These FRU values might display in this message for these switches, but these parts cannot be replaced separately. The entire switch is a FRU.

Recommended Action

Verify that the FRU was intended to be removed. replace the FRU as soon as possible.

Severity

INFO

EM-1051

Message

```
<timestamp>, [EM-1051], <sequence-number>,, INFO, <system-name>,  
<FRU Id>: Inconsistency detected, FRU re-initialized
```

Probable Cause

Indicates that an inconsistent state was found in the FRU. This occurs if the state of the FRU was changing during a failover. The FRU is reinitialized and traffic might have been disrupted.

Recommended Action

No action is required.

Severity

INFO

EM-1052

Message

```
<timestamp>, [EM-1052], <sequence-number>,, WARNING, <system-name>, <FRU Id>  
sensor 0x<Sensor Code> value out of range: <Raw Sensor Value>/<Retry Count>
```

Probable Cause

Indicates that one or more sensor values for a FRU are radically out of range. This might be a environmental problem or a problem with the sensor hardware.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- Switch for fixed port count switches.
- *Slot 1* through *Slot 10* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.
- *PS 1* through *PS 4* (power supplies) for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, or *PS 1* through *PS 2* for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *Fan 1* through *Fan 3* for the Core Switch 2/64, SAN Director 2/128, and SAN Switch 4/32 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *WWN 1* or *WWN 2* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.

The does not have any fans, power supplies or WWN cards.

The 4/8 SAN Switch, 4/16 SAN Switch has 4 fans and 1 power supply, but these parts cannot be replaced: the entire switch is a FRU. The 4/8 SAN Switch, 4/16 SAN Switch fans do not have RPM sensors, so cannot display fan speed.

This message can display:

- voltages in volts
- temperature in Celsius
- fan speeds in RPM

Recommended Action

If the message is isolated, it might be a transient problem with the sensor hardware; monitor the error messages on the switch. If the message is persistent, without other environmental errors, replace the FRU.

If the message is persistent, and there are other associated environmental messages, follow the actions for those messages.

Severity

WARNING

EM-1053

Message

```
<timestamp>, [EM-1053], <sequence-number>,, WARNING, <system-name>,  
No cached sensor values available for <FRU Id>
```

Probable Cause

Indicates that there are no cached sensor values for the sensor, and software was unable to read new values.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- Switch for fixed port count switches.
- *Slot 1* through *Slot 10* for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.
- *PS 1* through *PS 4* (power supplies) for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, or *PS 1* through *PS 2* for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- *Fan 1* through *Fan 3* for the Core Switch 2/64, SAN Director 2/128, and SAN Switch 4/32 (six fans in three FRUs). *Fan 1* through *Fan 6* for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.

The does not have any fans, power supplies or WWN cards.

The 4/8 SAN Switch, 4/16 SAN Switch has 4 fans and 1 power supply, but these parts cannot be replaced: the entire switch is a FRU. The 4/8 SAN Switch, 4/16 SAN Switch fans do not have RPM sensors, so cannot display fan speed.

Recommended Action

If the message is isolated, it might be a transient problem with the sensor hardware; monitor the error messages on the switch.

Try reseating the FRU. If the message persists, replace the FRU.

Severity

WARNING

EM-1055

Message

```
<timestamp>, [EM-1055], <sequence-number>,, WARNING, <system-name>, <FRU Id>: Port media incompatible. Reason: <Reason for incompatibility>
```

Probable Cause

Indicates that an incompatible port media is detected.

The possible causes are:

- The port media is not capable of running at the configured port speed.
- The port media generates too much heat to be used in the slot.

Recommended Action

Verify that the media can be run at the configured port speed.

If the port media is extended long wavelength, move it to a port that can support the heat generated.

Severity

WARNING

EM-1056

Message

```
<timestamp>, [EM-1056], <sequence-number>,, WARNING, <system-name>, <FRU Id>: Port faulted. Reason: <Reason code for the fault>
```

Probable Cause

Indicates a faulty port media is detected. The reason code for this message is for internal use only. This message is valid for only the SAN Switch 4/32.

Recommended Action

Replace the defective SFP.

Severity

WARNING

EM-1057

Message

```
<timestamp>, [EM-1057], <sequence-number>,, WARNING, <system-name>, Blade: <Slot Id> is getting reset: <fault Reason>
```

Probable Cause

Indicates the switch is getting an automatic reset. This is usually a transient problem.

Recommended Action

If the message is persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

EM-1058

Message

```
<timestamp>, [EM-1058], <sequence-number>,, WARNING, <system-name>, Switch gets  
reset: <fault reason>
```

Probable Cause

Indicates the switch is getting an automatic reset. This is usually a transient problem.

Recommended Action

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

EM-1059

Message

```
<timestamp>, [EM-1059], <sequence-number>,, CRITICAL, <system-name>, Incompatible unit  
in <FRU Id> faulted
```

Probable Cause

Indicates that a FRU inserted in the specified slot is not compatible with the switch software. The blade is faulted. This message only occurs on the Core Switch 2/64, SAN Director 2/128, or 4/256 SAN Director.

Recommended Action

Replace the blade. Verify that the replacement blade is compatible with your CP types and your **chassisConfig** option.

Severity

CRITICAL

EVMD error messages

EVMD-1001

Message

```
<timestamp>, [EVMD-1001], <sequence-number>,, WARNING,  
<system-name>, Event session killed, host IP = <Host IP address>,  
port = <Host TCP port number>
```

Probable Cause

The TCP socket is closed because of a TCP write error. There can be many causes for this loss of connection:

- The API host application exits without notifying the switch.

- The API host computer is shut down.
- There has been a network problem.
- The Ethernet cable is not properly connected to the switch.
- A user has unplugged the Ethernet cable and then plugged it back in.

Recommended Action

This problem can be transient; try to reestablish the connection.

If the cause is a network or Ethernet cable problem, you must fix the problem before you can reestablish an API session. Verify that your workstation has a TCP connection to the switch.

The Fabric OS automatically kills unused sessions to prevent resource leaking.

Severity

WARNING

FABS error messages

FABR-1001

Message

```
<timestamp>, [FABR-1001], <sequence-number>,, WARNING,
<system-name>, port <port number>, <segmentation reason>
```

Probable Cause

Indicates that the specified switch port is isolated because of a segmentation due to mismatched configuration parameters.

Recommended Action

Based on the segmentation reason displayed with the message, look for a possible mismatch of relevant configuration parameters in the switches at both ends of the link.

Run the **configure** command to modify the appropriate switch parameters on both the local and remote switch.

Severity

WARNING

FABR-1002

Message

```
<timestamp>, [FABR-1002], <sequence-number>,, WARNING,
<system-name>, fabGaid: no free multicast alias IDs
```

Probable Cause

Indicates that the fabric does not have any available multicast alias IDs to assign to the alias server.

Recommended Action

Verify alias IDs using the **fabricShow** command on the principal switch.

Severity

WARNING

FABR-1003

Message

```
<timestamp>, [FABR-1003], <sequence-number>,, WARNING,  
<system-name>, port <port number>: ILS <command> bad size <payload  
size>, wanted <expected payload size>
```

Probable Cause

Indicates that an internal link service (ILS) information unit of invalid size has been received. The neighbor switch has sent an invalid sized payload.

Recommended Action

Investigate the neighbor switch for problems. Run the **errShow** command on the neighbor switch to view the error log for additional messages.

Check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary.

Run the **portLogDumpPort** command on both the receiving and transmitting ports.

Run the **fabStateShow** command on both the receiving and transmitting switches.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

FABR-1004

Message

```
<timestamp>, [FABR-1004], <sequence-number>,, WARNING,  
<system-name>, port: <port number>, req iu: 0x<address of IU  
request sent>, state: 0x<command sent>, resp iu: 0x<address of  
response IU received>, state 0x<response IU state>, <additional  
description>
```

Probable Cause

Indicates that the information unit response was invalid for the specified command sent. The fabric received an unknown response. This message is rare and usually indicates a problem with the Fabric OS kernel.

Recommended Action

If this message is due to a one-time event because of the incoming data, the system will discard the frame. If it is due to problems with the kernel, the system will recover by performing a failover.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

FABR-1005

Message

```
<timestamp>, [FABR-1005], <sequence-number>,, WARNING,  
<system-name>, <command sent>: port <port number>: status 0x<reason  
for failure> (<description of failure reason>) xid = 0x<exchange ID  
of command>
```

Probable Cause

Indicates that the application failed to send an async command for the specified port. The message provides additional details regarding the reason for the failure and the exchange ID of the command. This can happen if a port is about to go down.

Recommended Action

This message is often transitory. No action is required.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

FABR-1006

Message

```
<timestamp>, [FABR-1006], <sequence-number>,, WARNING,  
<system-name>, Node free error, caller: <error description>
```

Probable Cause

Indicates that the Fabric OS is trying to free or deallocate memory space that has already been deallocated. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action

In case of severe memory corruption, the system might recover by performing an automatic failover.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

FABR-1007

Message

```
<timestamp>, [FABR-1007], <sequence-number>,, WARNING,  
<system-name>, IU free error, caller: <function attempting to  
de-allocate IU>
```

Probable Cause

Indicates that a failure occurred when deallocating an information unit. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action

In case of severe memory corruption, the system might recover by performing an automatic failover.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

FABR-1008

Message

```
<timestamp>, [FABR-1008], <sequence-number>,, WARNING,  
<system-name>, <error description>
```

Probable Cause

Indicates that errors occurred during the request domain ID state; the information unit cannot be allocated or sent. If this message occurs with FABR-1005, the problem is usually transitory. Otherwise, this message is rare and usually indicates a problem with the Fabric OS. The error descriptions are as follows:

- FAB RDI: cannot allocate IU
- FAB RDI: cannot send IU

Recommended Action

No action is required if the message appears with the FABR_1005 message.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

FABR-1009

Message

```
<timestamp>, [FABR-1009], <sequence-number>,, WARNING,  
<system-name>, <error description>
```

Probable Cause

Indicates that errors were reported during the exchange fabric parameter state; cannot allocate domain list due to a faulty EFP type. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action

The fabric daemon will discard the EFP. The system will recover through the EFP retrieval process.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

FABR-1010

Message

```
<timestamp>, [FABR-1010], <sequence-number>,, WARNING,  
<system-name>, <error description>
```

Probable Cause

Indicates that the errors occurred while cleaning up the RDI (request domain ID). The error description provides further details. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

FABR-1011

Message

```
<timestamp>, [FABR-1011], <sequence-number>,, ERROR, <system-name>,  
<error description>
```

Probable Cause

Indicates that the Fabric OS is unable to inform the FSSME (Fabric OS State Synchronization Management module) that the fabric is stable or unstable. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

FABR-1012

Message

```
<timestamp>, [FABR-1012], <sequence-number>,, WARNING,  
<system-name>, <function stream>: no such type, <invalid type>
```

Probable Cause

Indicates that the fabric is not in the appropriate state for the specified process. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action

The fabric daemon will take proper action to recover from the error.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

FABR-1013

Message

```
<timestamp>, [FABR-1013], <sequence-number>,, CRITICAL,  
<system-name>, No Memory: pid=<fabric process id> file=<source file  
name> line=<line number within the source file>
```

Probable Cause

Indicates that there is not enough memory in the switch for the fabric module to allocate. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action

The system will recover by failing over to the standby CP.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

CRITICAL

FABR-1014

Message

```
<timestamp>, [FABR-1014], <sequence-number>,, ERROR, <system-name>,  
Port <port number> Disabled: Insistent Domain ID <Domain ID> could  
not be obtained. Principal Assigned Domain ID = <Domain ID>
```

Probable Cause

Indicates that the specified port received an RDI (request domain ID) accept message containing a principal-switch-assigned domain ID that is different from the insistent domain ID (IDID). FICON mode requires an insistent domain ID. If an RDI response has a different domain ID, then the port is disabled.

Recommended Action

Run the **configShow** command to view the fabric.ididmode. A 0 means the IDID mode is disabled; a 1 means it is enabled.

Set the switch to insistent domain ID mode. This mode is set under the **configure** command or in Web Tools on the **Switch Admin > configure** window.

Severity

ERROR

FABR-1015

Message

```
<timestamp>, [FABR-1015], <sequence-number>,, ERROR, <system-name>,  
FICON Insistent DID max retry exceeded: All E-Ports will be  
disabled. Switch is isolated.
```

Probable Cause

Indicates that the application exceeded RDI (request domain ID) requests for the insistent domain ID. All E_Ports are disabled, isolating the specified switch from the fabric.

Recommended Action

Verify that the insistent domain ID is unique in the fabric and then reenables the E_Ports. Run the **fabricShow** command to view the domain IDs across the fabric and the **configure** command to change the insistent domain ID mode. Refer to the *HP StorageWorks Fabric OS 5.x command reference guide* for more information on these commands.

Severity

ERROR

FABR-1016

Message

```
<timestamp>, [FABR-1016], <sequence-number>,, WARNING,  
<system-name>, ficonMode is enabled.
```

Probable Cause

Indicates that FICON mode is enabled on the switch through a user interface command.

Recommended Action

No action is required.

Severity

WARNING

FABR-1017

Message

```
<timestamp>, [FABR-1017], <sequence-number>,, WARNING,  
<system-name>, ficonMode is disabled.
```

Probable Cause

Indicates that FICON mode is disabled on the switch through a user interface command.

Recommended Action

No action is required.

Severity

WARNING

FABR-1018

Message

```
<timestamp>, [FABR-1018], <sequence-number>,, WARNING,  
<system-name>, PSS principal failed (<reason for not becoming the  
principal switch>: <WWN of new principal switch>)
```

Probable Cause

Indicates that a failure occurred when trying to set the principal switch using the **fabricPrincipal** command. The message notifies the user that the switch failed to become the principal switch because either:

- The switch joined an existing fabric and bypassed the F0 state.
- The fabric already contains a principal switch that has a lower WWN.

Recommended Action

Make sure that no other switches is configured as the principal switch. Force a fabric rebuild by using the **switchDisable** and **switchEnable** commands.

Refer to the *HP StorageWorks Fabric OS 5.x command reference guide* for more information the **fabricPrincipal** command.

Severity

WARNING

FABR-1019

Message

```
<timestamp>, [FABR-1019], <sequence-number>,, CRITICAL,  
<system-name>, Critical fabric size (<current domains>) exceeds  
supported configuration (<supported domains>)
```

Probable Cause

Indicates that this switch is a value-line switch and has exceeded the limited fabric size: that is, a specified limit to the number of domains. This limit is defined by your specific value-line license key. The fabric size has exceeded this specified limit, and the grace period counter has started. If the grace period is complete and the size of the fabric is still outside the specified limit, Web Tools is disabled.

Recommended Action

Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

Severity

CRITICAL

FABR-1020

Message

```
<timestamp>, [FABR-1020], <sequence-number>,, CRITICAL,  
<system-name>, Webtool will be disabled in <days> days <hours>  
hours and <minutes> minutes
```

Probable Cause

Indicates that this switch has a value-line license and has a limited number of domains. If more than the specified number of domains are in the fabric, a counter is started to disable Web Tools. This message displays the number of days left in the grace period. After this time, Web Tools is disabled.

Recommended Action

Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

Severity

CRITICAL

FABR-1021

Message

```
<timestamp>, [FABR-1021], <sequence-number>,, CRITICAL,  
<system-name>, Webtool is disabled
```

Probable Cause

Indicates that this switch has a value-line license and has a limited number of domains. If more than the specified number of domains are in the fabric, a counter is started to disable Web Tools. This grace period has expired and Web Tools has been disabled.

Recommended Action

Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

Severity

CRITICAL

FABR-1022

Message

```
<timestamp>, [FABR-1022], <sequence-number>,, CRITICAL,  
<system-name>, Fabric size (<actual domains>) exceeds supported  
configuration (<supported domains>). Fabric limit timer (<type>)  
started from <grace period in seconds>.
```

Probable Cause

Indicates that the fabric size has exceeded the value-line limit, and the grace period counter has started. If the grace period is complete and the size of the fabric is still outside the specified limit, Web Tools is disabled.

Recommended Action

Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

Severity

CRITICAL

FABR-1023

Message

```
<timestamp>, [FABR-1023], <sequence-number>,, INFO, <system-name>,  
Fabric size is within supported configuration (<supporteddomains>).  
Fabric limit timer (<type>) stopped at <grace period in seconds>.
```

Probable Cause

Indicates that the fabric size is within specified limits. Either a full fabric license was added or the size of the fabric was changed to within the licensed limit.

Recommended Action

No action is required.

Severity

INFO

FABR-1024

Message

```
<timestamp>, [FABR-1024], <sequence-number>,, INFO, <system-name>,  
Initializing fabric size limit timer <grace period>
```

Probable Cause

Indicates that the fabric size has exceeded the limit set by your value-line switches. Value-line switches have a limited fabric size: a specified limit to the number of domains. This value is defined by your specific value-line license key. The fabric size has exceeded this specified limit. The grace-period timer has been initialized. If the grace period is complete and the size of the fabric is still outside the specified limit, Web Tools is disabled.

Recommended Action

Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

Severity

INFO

FABR-1029

Message

```
<timestamp>, [FABR-1029], <sequence-number>,, INFO, <system-name>,  
Port <port number> negotiated <flow control mode description> (mode  
= <received flow control mode>)
```

Probable Cause

Indicates that a different flow control mode, as described in the message, is negotiated with the port at the other end of the link. The flow control is a mechanism of throttling the transmitter port to avoid buffer overrun at the receiving port. There are three types of flow control modes:

- VC_RDY mode: Virtual-channel flow control mode. This is a proprietary protocol.

- R_RDY mode: Receiver-ready flow control mode. This is the Fibre Channel standard protocol, that uses R_RDY primitive for flow control.
- DUAL_CR mode: Dual-credit flow control mode. In both of the previous modes, the buffer credits are fixed, based on the port configuration information. In this mode, the buffer credits are negotiated as part of ELP exchange. This mode also uses the R_RDY primitive for flow control.

Recommended Action

No action is required.

Severity

INFO

FABR-1030

Message

```
<timestamp>, [FABR-1030], <sequence-number>,, INFO, <system-name>,
fabric: Domain <new domain ID> (was <old domain ID>)
```

Probable Cause

Indicates that the domain ID for a switch has been changed.

Recommended Action

No action is required.

Severity

INFO

FABS-1001

Message

```
<timestamp>, [FABS-1001], <sequence-number>,, CRITICAL,
<system-name>, <Function name> <Description of memory need>
```

Probable Cause

Indicates that the system is low on memory and cannot allocate more memory for new operations. This is usually an internal Fabric OS problem or file corruption. *Description of memory need* indicates how much memory was being requested. The value could be any whole number.

Recommended Action

Reboot or power cycle the switch.

Severity

CRITICAL

FABS-1002

Message

```
<timestamp>, [FABS-1002], <sequence-number>,, WARNING,
<system-name>, <Function name> <Description of problem>
```

Probable Cause

Indicates that an internal problem has been detected by the software. This is usually an internal Fabric OS problem or file corruption.

Recommended Action

Reboot or power cycle the switch.

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity

WARNING

FABS-1004

Message

```
<timestamp>, [FABS-1004], <sequence-number>,, WARNING,  
<system-name>, <Function name and description of problem> process  
<Process ID number> (<Current command name>) <Pending signal  
number>
```

Probable Cause

Indicates that an operation has been interrupted by a signal. This is usually an internal Fabric OS problem or file corruption.

Recommended Action

Reboot or power cycle the switch.

Severity

WARNING

FABS-1005

Message

```
<timestamp>, [FABS-1005], <sequence-number>,, WARNING,  
<system-name>, <Function name and description of problem> (<ID  
type>= <ID number>)
```

Probable Cause

Indicates that an unsupported operation has been requested. This is usually an internal Fabric OS problem or file corruption. The possible values for *function name and description of problem* are:

fabsys_write: Unsupported write operation: process xxx

where xxx is the process ID (PID), which could be any whole number.

Recommended Action

Reboot or power cycle the active CP (for modular systems) or the switch (for single-board systems).

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity

WARNING

FABS-1006

Message

```
<timestamp>, [FABS-1006], <sequence-number>,, WARNING,  
<system-name>, <Function name and description of problem>: object  
<object type id> unit <slot>
```

Probable Cause

Indicates that there is no device in the slot with the specified object type ID in the system module record. This could indicate that a serious Fabric OS data problem on the switch. The possible values for *function name and description of problem* are:

- setSoftState: bad object
- setSoftState: invalid type or unit
- media_sync: Media oid mapping failed
- fabsys_media_i2c_op: Media oid mapping failed
- fabsys_media_i2c_op: obj is not media type
- media_class_hndlr: failed sending media state to blade driver

Recommended Action

If the message is isolated, monitor the error messages on the switch. If the error is repetitive or if the fabric failed, fail over or reboot the switch.

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity

WARNING

FABS-1007

Message

```
<timestamp>, [FABS-1007], <sequence-number>,, WARNING,  
<system-name>, <Function name>: Media state is invalid -  
status=<Status value>
```

Probable Cause

Indicates that the Fabric OS has detected an invalid value in an object's status field. This is usually an internal Fabric OS problem or file corruption.

Recommended Action

Reboot or power cycle the switch.

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity

WARNING

FABS-1008

Message

```
<timestamp>, [FABS-1008], <sequence-number>,, WARNING,  
<system-name>, <Function name>: Media oid mapping failed
```

Probable Cause

Indicates that the Fabric OS was unable to locate a necessary object handle. This is usually an internal Fabric OS problem or file corruption.

Recommended Action

Reboot or power cycle the switch.

Severity

WARNING

FABS-1009

Message

```
<timestamp>, [FABS-1009], <sequence-number>,, WARNING,  
<system-name>, <Function name>: type is not media
```

Probable Cause

Indicates that the Fabric OS was unable to locate an appropriate object handle. This is usually an internal Fabric OS problem or file corruption.

Recommended Action

Reboot or power cycle the switch.

Severity

WARNING

FABS-1010

Message

```
<timestamp>, [FABS-1010], <sequence-number>,, WARNING,  
<system-name>, <Function name>: Wrong media_event <Event number>
```

Probable Cause

Indicates that the Fabric OS detected an unknown event type. This is usually an internal Fabric OS problem or file corruption.

Recommended Action

Reboot or power cycle the switch.

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity

WARNING

FABS-1011

Message

```
<timestamp>, [FABS-1011], <sequence-number>,, ERROR, <system-name>,  
<Method name>[<Method tag number>]:Invalid input state 0x<Input  
state code>
```

Probable Cause

An unrecognized state code was used in an internal Fabric OS message for a FRU.

Recommended Action

Reboot or power-cycle the CP or system.

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity

ERROR

FABS-1012

Message

```
<timestamp>, [FABS-1012], <sequence-number>,, ERROR, <system-name>,  
<Method name>[<Method tag number>]:FRU state transition failed.  
Current state 0x<Current state of FRU> Requested state 0x<Requested  
new state of FRU> err 0x<Error code>
```

Probable Cause

A FRU could not be transitioned to the requested state. This is usually an internal Fabric OS problem.

Recommended Action

Reboot or power-cycle the CP or system.

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity

ERROR

FABS-1013

Message

```
<timestamp>, [FABS-1013], <sequence-number>,, ERROR, <system-name>,  
<Method name>[<Method tag number>]:Unknown blade type 0x<Blade  
type>
```

Probable Cause

An unrecognized type of blade has been discovered in the system.

This may be caused by an incorrect FRU header, inability to read the FRU header, or the blade may not be supported by this platform or Fabric OS version.

Recommended Action

Verify that the blade is valid for use in this system and this version of Fabric OS

Try reseating the blade

If this is a valid blade and reseating doesn't help, then replace the blade

Severity

ERROR

FABS-1014

Message

```
<timestamp>, [FABS-1014], <sequence-number>,, ERROR, <system-name>,  
<Method name>[<Method tag number>]:Unknown FRU type 0x<FRU Object  
type>
```

Probable Cause

An unrecognized of FRU has been discovered in the system.

This may be caused by an incorrect FRU header, inability to read the FRU header, or the FRU may not be supported by this platform or Fabric OS version.

Recommended Action

Verify that the FRU is valid for use in this system and this version of Fabric OS

Try reseating the FRU

If this is a valid FRU and reseating doesn't help, then replace the FRU

Severity

ERROR

FABS-1015

Message

```
<timestamp>, [FABS-1015], <sequence-number>,, ERROR, <system-name>,  
<Method name>[<Method tag number>]:Request to enable FRU type  
0x<FRU Object type>, unit <Unit number> failed. err code <Error  
code>
```

Probable Cause

Indicates the specified FRU could not be enabled. This is usually an internal Fabric OS problem.

Recommended Action

Try removing and reinserting the FRU.

Reboot or power-cycle the CP or system.

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity

ERROR

FCMC error messages

FCMC-1001

Message

```
<timestamp>, [FCMC-1001], <sequence-number>,, CRITICAL,  
<system-name>, <function>: <failed function call> failed, out of  
memory condition
```

Probable Cause

Indicates that the switch is low on memory and failed to allocate new memory for an information unit (IU).

Recommended Action

A nonbladed switch will automatically reboot. For a bladed switch, the active CP blade will automatically fail over and the standby CP will become the active CP.

Severity

CRITICAL

FCPD error messages

FCPD-1001

Message

```
<timestamp>, [FCPD-1001], <sequence-number>,, WARNING,  
<system-name>, Probing failed on <error string>
```

Probable Cause

Indicates that an FCP switch probed devices on a loop port, and probing failed on either the L_Port, AL_PA address, or the F_Port. For the AL_PA, the valid range is 00 through FF. The error string can be either:

- L_Port *port_number* ALPA *alpa_number*
- F_Port *port_number*

Recommended Action

This can happen when the firmware on the device controller on the specified port has a defect. Check with the device vendor for a firmware upgrade containing a defect fix.

The SAN Switch 4/32 does not support private loop devices.

Severity

WARNING

FCPD-1002

Message

```
<timestamp>, [FCPD-1002], <sequence-number>,, WARNING,  
<system-name>, port <port number>, bad R_CTL for fcp probing:  
0x<R_CTL value>
```


Probable Cause

Indicates that the response frame received on the specified port for a inquiry request contains an invalid value in the routing control field.

Recommended Action

This can happen only if the firmware on the device controller on the specified port has a defect. Check with the device vendor for a firmware upgrade containing a defect fix.

Severity

WARNING

FCPD-1003

Message

```
<timestamp>, [FCPD-1003], <sequence-number>,, INFO, <system-name>,  
Probing failed on <error string> which is possibly a private device  
which is not supported in this port type
```

Probable Cause

Private devices will not respond to the switch PLOGI during probing.

Recommended Action

Refer to the switch vendor for a list of other port types that support private devices for inclusion into the fabric.

Severity

INFO

FCPH error messages

FCPH-1001

Message

```
<timestamp>, [FCPH-1001], <sequence-number>,, CRITICAL,  
<system-name>, <function>: <failed function call> failed, out of  
memory condition
```

Probable Cause

Indicates that the switch is low on memory and failed to allocate new memory for a Fibre Channel driver instance.

The *function* can only be `fc_create`. This function creates a Fibre Channel driver instance.

The *failed function call* is `kmalloc_wrapper` failed. This function call is for kernel memory allocation.

Recommended Action

A nonbladed switch will automatically reboot. For a bladed switch, the active CP blade will automatically fail over, and the standby CP will become the active CP.

Severity

CRITICAL

FICU error messages

FICU-1001

Message

```
<timestamp>, [FICU-1001], <sequence-number>,, ERROR, <system-name>,  
<function name>: config<config Set(key)|Get(key)| Save> failed rc =  
<error>
```

Probable Cause

Indicates that one of the configuration management functions failed. The key variable is part of the Fabric OS configuration database and is for support use only. The error variable is an internal error number.

Recommended Action

Execute an **haFailover** on the switch if it has redundant CPs or reboot the switch. Run the **saveCore** command to check if your flash is full. If the flash is full, run the **saveCore** command to clear the core files. Refer to the *HP StorageWorks Fabric OS 5.x command reference guide* for more information on these commands.

Severity

ERROR

FICU-1002

Message

```
<timestamp>, [FICU-1002], <sequence-number>,, ERROR, <system-name>,  
Failed to get RNID from Management Server Domain=<domain>  
rc=<error>
```

Probable Cause

Indicates that the FICON-CUP daemon failed to get switch RNID from the management server due to a Fabric OS problem. The domain variable displays the domain ID of the target switch for this RNID. The error variable is an internal error number.

Recommended Action

If this is a bladed switch, execute the **haFailover** command. If the problem persists, or if this is a nonbladed switch, download a new firmware version using the **firmwareDownload** command. Refer to the *HP StorageWorks Fabric OS 5.x command reference guide* for more information on this command.

Severity

ERROR

FICU-1003

Message

```
<timestamp>, [FICU-1003], <sequence-number>,, WARNING,  
<system-name>, <function name>: <message> FICON-CUP License Not  
Installed (<error>)
```

Probable Cause

Indicates that the FICON-CUP license is not installed on the switch.

Recommended Action

Run the **licenseShow** command to check the installed licenses on the switch. The switch cannot be managed using FICON-CUP commands until the FICON-CUP license is installed. Contact your switch supplier for a FICON-CUP license. Run the **licenseAdd** command to add the license to your switch.

Severity

WARNING

FICU-1004

Message

```
<timestamp>, [FICU-1004], <sequence-number>,, WARNING,  
<system-name>, <function name>: Failed to set FMS mode: conflicting  
PID Format:<pid_format>, FMS Mode:<mode>
```

Probable Cause

Indicates that a PID format conflict was encountered. The core PID format is required for FICON-CUP.

The pid_format variable displays the PID format currently running on the fabric:

- 0 is VC-encoded PID format
- 1 is core PID format
- 2 is extended-edge PID format

FMS mode displays whether FICON Management Server mode is enabled; a 0 means this mode is enabled and a 1 means this mode is disabled.

Recommended Action

For FICON Management Server mode (fmsmode) to be enabled, the core PID format must be used in the fabric. Change the PID format to core PID using the **configure** command and reenables fmsmode using **ficoncupset** command. Refer to the *HP StorageWorks Fabric OS 5.x administrator guide* for information on core PID mode and the HP StorageWorks Fabric OS 5.x command reference guide for information on the **configure** command and **ficoncupset** command.

Severity

WARNING

FICU-1005

Message

```
<timestamp>, [FICU-1005], <sequence-number>,, ERROR, <system-name>,  
Failed to initialize <module> rc = <error>
```

Probable Cause

Indicates that an initialization of a module within the FICON-CUP daemon failed.

Recommended Action

Download a new firmware version using the **firmwareDownload** command. Refer to the *HP StorageWorks Fabric OS 5.x command reference guide* for more information on this command.

Severity

ERROR

FICU-1006

Message

```
<timestamp>, [FICU-1006], <sequence-number>,, WARNING,  
<system-name>, Control Device Allegiance Reset (Logical Path:  
0x<PID>:0x<channel image ID>)
```

Probable Cause

Indicates that the path with the specified PID and channel image ID lost allegiance to a FICON-CUP device.

Recommended Action

Check if the FICON channel corresponding to the PID in the message is functioning correctly.

Severity

WARNING

FICU-1007

Message

```
<timestamp>, [FICU-1007], <sequence-number>,, WARNING,  
<system-name>, <function name>: Failed to allocate memory while  
performing <message>
```

Probable Cause

Indicates that memory resources are low. This might be a transient problem.

Recommended Action

If the message persists, check the memory usage on the switch, using the **memShow** command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

FICU-1008

Message

```
<timestamp>, [FICU-1008], <sequence-number>,, WARNING,  
<system-name>, FMS mode has been enabled. Port:<port number> has  
been disabled due to port address conflict.
```

Probable Cause

Indicates that the specified port was disabled when the switch was enabled for FICON Management Server mode (fmsmode). This was due to a port address conflict.

Recommended Action

No action is required.

Severity

WARNING

FICU-1009

Message

```
<timestamp>, [FICU-1009], <sequence-number>,, WARNING,  
<system-name>, FMS Mode enable failed due to insufficient frame  
filtering resources on some ports
```

Probable Cause

Indicates that the frame filtering resources required to enable FICON Management Server mode (fmsmode) were not available on some of the ports.

Recommended Action

Use the **perfDelFilterMonitor** command to delete the filter-based performance monitors used on all ports to free up the resources.

Severity

WARNING

FKLB error messages

FICU-1001

Message

```
<timestamp>, [FICU-1001], <sequence-number>,, ERROR, <system-name>,  
<function name>: config<config Set(key)|Get(key)| Save> failed rc =  
<error>
```

Probable Cause

Indicates that one of the configuration management functions failed. The key variable is part of the Fabric OS configuration database and is for support use only. The error variable is an internal error number.

Recommended Action

Execute an **haFailover** on the switch if it has redundant CPs or reboot the switch. Run the **saveCore** command to check if your flash is full. If the flash is full, run the **saveCore** command to clear the core files. Refer to the *HP StorageWorks Fabric OS 5.x command reference guide* for more information on these commands.

Severity

ERROR

FICU-1002

Message

```
<timestamp>, [FICU-1002], <sequence-number>,, ERROR, <system-name>,  
Failed to get RNID from Management Server Domain=<domain>  
rc=<error>
```

Probable Cause

Indicates that the FICON-CUP daemon failed to get switch RNID from the management server due to a Fabric OS problem. The domain variable displays the domain ID of the target switch for this RNID. The error variable is an internal error number.

Recommended Action

If this is a bladed switch, execute the **haFailover** command. If the problem persists, or if this is a nonbladed switch, download a new firmware version using the **firmwareDownload** command. Refer to the *HP StorageWorks Fabric OS 5.x command reference guide* for more information on this command.

Severity

ERROR

FICU-1003

Message

```
<timestamp>, [FICU-1003], <sequence-number>,, WARNING,  
<system-name>, <function name>: <message> FICON-CUP License Not  
Installed (<error>)
```

Probable Cause

Indicates that the FICON-CUP license is not installed on the switch.

Recommended Action

Run the **licenseShow** command to check the installed licenses on the switch. The switch cannot be managed using FICON-CUP commands until the FICON-CUP license is installed. Contact your switch supplier for a FICON-CUP license. Run the **licenseAdd** command to add the license to your switch.

Severity

WARNING

FICU-1004

Message

```
<timestamp>, [FICU-1004], <sequence-number>,, WARNING,  
<system-name>, <function name>: Failed to set FMS mode: conflicting  
PID Format:<pid_format>, FMS Mode:<mode>
```

Probable Cause

Indicates that a PID format conflict was encountered. The core PID format is required for FICON-CUP.

The `pid_format` variable displays the PID format currently running on the fabric:

- 0 is VC-encoded PID format
- 1 is core PID format
- 2 is extended-edge PID format

FMS mode displays whether FICON Management Server mode is enabled; a 0 means this mode is enabled and a 1 means this mode is disabled.

Recommended Action

For FICON Management Server mode (`fmsmode`) to be enabled, the core PID format must be used in the fabric. Change the PID format to core PID using the **configure** command and reenables `fmsmode` using **ficoncupset** command. Refer to the *HP StorageWorks Fabric OS 5.x administrator guide* for information

on core PID mode and the HP StorageWorks Fabric OS 5.x command reference guide for information on the **configure** command and **ficoncupset** command.

Severity

WARNING

FICU-1005

Message

```
<timestamp>, [FICU-1005], <sequence-number>,, ERROR, <system-name>,  
Failed to initialize <module> rc = <error>
```

Probable Cause

Indicates that an initialization of a module within the FICON-CUP daemon failed.

Recommended Action

Download a new firmware version using the **firmwareDownload** command. Refer to the *HP StorageWorks Fabric OS 5.x command reference guide* for more information on this command.

Severity

ERROR

FICU-1006

Message

```
<timestamp>, [FICU-1006], <sequence-number>,, WARNING,  
<system-name>, Control Device Allegiance Reset (Logical Path:  
0x<PID>:0x<channel image ID>)
```

Probable Cause

Indicates that the path with the specified PID and channel image ID lost allegiance to a FICON-CUP device.

Recommended Action

Check if the FICON channel corresponding to the PID in the message is functioning correctly.

Severity

WARNING

FICU-1007

Message

```
<timestamp>, [FICU-1007], <sequence-number>,, WARNING,  
<system-name>, <function name>: Failed to allocate memory while  
performing <message>
```

Probable Cause

Indicates that memory resources are low. This might be a transient problem.

Recommended Action

If the message persists, check the memory usage on the switch, using the **memShow** command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

FICU-1008

Message

```
<timestamp>, [FICU-1008], <sequence-number>,, WARNING,  
<system-name>, FMS mode has been enabled. Port:<port number> has  
been disabled due to port address conflict.
```

Probable Cause

Indicates that the specified port was disabled when the switch was enabled for FICON Management Server mode (fmsmode). This was due to a port address conflict.

Recommended Action

No action is required.

Severity

WARNING

FICU-1009

Message

```
<timestamp>, [FICU-1009], <sequence-number>,, WARNING,  
<system-name>, FMS Mode enable failed due to insufficient frame  
filtering resources on some ports
```

Probable Cause

Indicates that the frame filtering resources required to enable FICON Management Server mode (fmsmode) were not available on some of the ports.

Recommended Action

Use the **perfDelFilterMonitor** command to delete the filter-based performance monitors used on all ports to free up the resources.

Severity

WARNING

FICU-1010

Message

```
<timestamp>, [FICU-1010], <sequence-number>,, WARNING,  
<system-name>, FMS Mode enable failed due to address conflict with  
port <port number>.
```

Probable Cause

Indicates that the FICON Management Server mode (fmsmode) was not enabled because the specified port has an address conflict with the CUP management port.

Recommended Action

Use the **portDisable** command to disable the specified port causing the address conflict.

Severity

WARNING

FLOD error messages

FLOD-1001

Message

```
<timestamp>, [FLOD-1001], <sequence-number>,, WARNING,  
<system-name>, Unknown LSR type: port <port number>, type <LSR  
header type>
```

Probable Cause

Indicates that the link state record (LSR) type is unknown. The following two LSR header types are the only known types: 1 - Unicast and 3 - Multicast.

Recommended Action

No action is required. The record is discarded.

Severity

WARNING

FLOD-1003

Message

```
<timestamp>, [FLOD-1003], <sequence-number>,, WARNING,  
<system-name>, Link count exceeded in received LSR, value = <link  
count number>
```

Probable Cause

Indicates that the acceptable link count received was exceeded in the link state record (LSR).

Recommended Action

No action is required. The record is discarded.

Severity

WARNING

FLOD-1004

Message

```
<timestamp>, [FLOD-1004], <sequence-number>,, ERROR, <system-name>,  
Excessive LSU length = <LSU length>
```

Probable Cause

Indicates that the LSU size exceeds what the system can support.

Recommended Action

Reduce the number of switches in the fabric or reduce the number of redundant ISLs between two switches.

Severity

ERROR

FLOD-1005

Message

```
<timestamp>, [FLOD-1005], <sequence-number>,, WARNING,  
<system-name>, Invalid received domain ID: <domain number>
```

Probable Cause

Indicates that the received LSR contained an invalid domain number. The switch will correct this condition automatically.

Recommended Action

No action is required. The LSR is discarded.

Severity

WARNING

FLOD-1006

Message

```
<timestamp>, [FLOD-1006], <sequence-number>,, WARNING,  
<system-name>, Transmitting invalid domain ID: <domain number>
```

Probable Cause

Indicates that the transmit LSR contained an invalid domain number.

Recommended Action

No action is required. The LSR is discarded.

Severity

WARNING

FSPF error messages

FSPF-1001

Message

```
<timestamp>, [FSPF-1001], <sequence-number>,, ERROR, <system-name>,  
Input Port <port number> out of range
```

Probable Cause

Indicates that the specified input port number is out of range; it does not exist on the switch.

Recommended Action

No action is required.

Severity

ERROR

FSPF-1002

Message

```
<timestamp>, [FSPF-1002], <sequence-number>,, INFO, <system-name>,  
Wrong neighbor ID (<domain ID>) in Hello message from port <port  
number>, expected ID = <domain ID>
```

Probable Cause

Indicates that the switch received the wrong domain ID from a neighbor (adjacent) switch in the HELLO message from a specified port. This might happen when a domain ID for a switch has been changed.

Recommended Action

No action is required.

Severity

INFO

FSPF-1003

Message

```
<timestamp>, [FSPF-1003], <sequence-number>,, ERROR, <system-name>,  
Remote Domain ID <domain number> out of range, input port = <port  
number>
```

Probable Cause

Indicates that the specified remote domain ID is out of range. The valid range is 1 through 239, except when **interopMode** is enabled, in which case the valid range is 97 to 127.

Recommended Action

No action is required. The frame is discarded.

Severity

ERROR

FSPF-1005

Message

```
<timestamp>, [FSPF-1005], <sequence-number>,, ERROR, <system-name>,  
Wrong Section Id <section number>, should be <section number>,  
input port = <port number>
```

Probable Cause

Indicates that an incorrect section ID was reported from the specified input port. The section ID is used to identify a set of switches that share an identical topology database. The section ID is implemented inside the protocol. The error message itself will indicate the mismatched section ID. It should be set to 0 for a nonhierarchical fabric. switches support only section ID 0.

Recommended Action

Use a frame analyzer to verify that the reported section ID is 0. Any connected (other manufacturer) switch with a section ID other than 0 is incompatible in a fabric of switches. Disconnect the offending switch.

Severity

ERROR

FSPF-1006

Message

```
<timestamp>, [FSPF-1006], <sequence-number>,, ERROR, <system-name>,  
FSPF Version <FSFP version> not supported, input port = <port  
number>
```

Probable Cause

Indicates that the FSPF version is not supported on the specified input port.

Recommended Action

Update the FSPF version by running the **firmwareDownload** command to update the firmware to the latest version. All current versions of the Fabric OS support FSPF version 2, which is the correct version.

Severity

ERROR

FSS error messages

FSS-1001

Message

```
<timestamp>, [FSS-1001], <sequence-number>,, WARNING,  
<system-name>, Application dropping HA data update.
```

Probable Cause

Indicates that an application has dropped a high availability (HA) data update.

Recommended Action

Run the **haSyncStart** command if this is a dual-CP system, or reboot the switch if it is a nonbladed system. The **haSyncStart** command will automatically run the **haSyncStop** command if required.

If the message persists, run **supportFtp** and **traceFtp -e** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

FSS-1002

Message

```
<timestamp>, [FSS-1002], <sequence-number>,, WARNING,  
<system-name>, Application sending too many concurrent HA data  
updates
```

Probable Cause

Indicates that an application has sent too many concurrent high availability (HA) data updates.

Recommended Action

Run the **haSyncStart** command if this is a dual-CP system, or reboot the switch if it is a nonbladed system. The **haSyncStart** command will automatically run the **haSyncStop** command if required.

If the message persists, run **supportFtp** and **traceFtp -e** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

FSS-1003

Message

```
<timestamp>, [FSS-1003], <sequence-number>,, WARNING,  
<system-name>, Application missing first HA data update
```

Probable Cause

Indicates that the FSS has dropped the update because an application has not set the transaction flag correctly.

Recommended Action

Run the **haSyncStart** command if this is a dual-CP system, or reboot the switch if it is a nonbladed system. The **haSyncStart** command will automatically run the **haSyncStop** command if required.

If the message persists, run **supportFtp** and **traceFtp -e** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

FSS-1004

Message

```
<timestamp>, [FSS-1004], <sequence-number>,, ERROR, <system-name>,  
Memory shortage
```

Probable Cause

Indicates that the system ran out of memory.

Recommended Action

Run the **memShow** command to view memory usage.

Run the **haSyncStart** command if this is a dual-CP system, or reboot the switch if it is a nonbladed system. The **haSyncStart** command will automatically run the **haSyncStop** command if required.

If the message persists, run **supportFtp** and **traceFtp -e** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

FSS-1005

Message

```
<timestamp>, [FSS-1005], <sequence-number>, , WARNING,  
<system-name>, FSS read failure
```

Probable Cause

Indicates that the read system call to the FSS device failed.

Recommended Action

If the message persists, run **supportFtp** and **traceFtp -e** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

FSS-1006

Message

```
<timestamp>, [FSS-1006], <sequence-number>, , WARNING,  
<system-name>, No message available
```

Probable Cause

Indicates that data is not available on the FSS device.

Recommended Action

If the message persists, run **supportFtp** and **traceFtp -e** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

FSSM errors

FSSM-1002

Message

```
<timestamp>, [FSSM-1002], <sequence-number>, , INFO, <system-name>,  
HA State is in sync
```

Probable Cause

Indicates that the HA state for the active CP is in synchronization with the HA state of the standby CP. If the standby CP is healthy, then a failover is nondisruptive. For more information on the **haFailover** command, refer to the *HP StorageWorks Fabric OS 5.x command reference guide*.

Recommended Action

No action is required.

Severity

INFO

FSSM-1003

Message

```
<timestamp>, [FSSM-1003], <sequence-number>,, WARNING,  
<system-name>, HA State out of sync
```

Probable Cause

Indicates that the HA state for the active CP is out of synchronization with the HA state of the standby CP. If the active CP failover occurs when the HA state is out of sync, the failover is disruptive.

Recommended Action

If this message was logged as a result of a user-initiated action (such as running the **switchReboot** command), then no action is required.

Otherwise, issue the **haSyncStart** command on the active CP and try resynchronizing the HA state.

If the HA state does not become synchronized, run the **haDump** command to help diagnose the problem.

If the message persists, run **supportFtp** and **traceFtp -e** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

FSSM-1004

Message

```
<timestamp>, [FSSM-1004], <sequence-number>,, INFO, <system-name>,  
Incompatible software version in HA synchronization.
```

Probable Cause

Indicates that the active CP and the standby CP in a dual CP system are running firmware that are incompatible with each other. If the active CP fails, the failover will be disruptive. In a pizza box system, this message is logged when firmware upgrade/downgrade was invoked. The new firmware version is not compatible with current running version. This cause a disruptive firmware upgrade/downgrade

Recommended Action

For a dual CP system, run the **firmwareDownload** command to load compatible firmware on the standby CP. For details on this command, refer to the *HP StorageWorks Fabric OS 5.x command reference guide*.

Severity

INFO

FW error messages

FW-1001

Message

```
<timestamp>, [FW-1001], <sequence-number>,, INFO, <system-name>,  
<label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the internal temperature of the switch has changed.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. To prevent recurring messages, disable the changed alarm for this threshold. If you receive a temperature-related message, check for an accompanying fan-related message and check fan performance. If all fans are functioning normally, check the climate control in your lab.

Severity

INFO

FW-1002

Message

```
<timestamp>, [FW-1002], <sequence-number>,, WARNING, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the internal temperature of the switch has fallen below the low boundary.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Typically, low temperatures means that the fans and airflow of a switch are functioning normally.

Verify that the location temperature is within the operational range of the switch. Refer to the hardware reference manual for the environmental temperature range of your switch.

Severity

WARNING

FW-1003

Message

```
<timestamp>, [FW-1003], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the internal temperature of the switch has risen above the high boundary to a value that might damage the switch.

Recommended Action

This message generally appears when a fan fails. If so, a fan-failure message accompanies this message. Replace the fan.

Severity

WARNING

FW-1004

Message

```
<timestamp>, [FW-1004], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the internal temperature of the switch has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. If you receive a temperature-related message, check for an accompanying fan-related message and check fan performance. If all fans are functioning normally, check the climate control in your lab.

Severity

INFO

FW-1005

Message

```
<timestamp>, [FW-1005], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the speed of the fan has changed. Fan problems typically contribute to temperature problems.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Consistently abnormal fan speeds generally indicate that the fan is malfunctioning.

Severity

INFO

FW-1006

Message

```
<timestamp>, [FW-1006], <sequence-number>,, WARNING, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the speed of the fan has fallen below the low boundary. Fan problems typically contribute to temperature problems.

Recommended Action

Consistently abnormal fan speeds generally indicate that the fan is failing. Replace the fan FRU.

Severity

WARNING

FW-1007

Message

```
<timestamp>, [FW-1007], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the speed of the fan has risen above the high boundary. Fan problems typically contribute to temperature problems.

Recommended Action

Consistently abnormal fan speeds generally indicate that the fan is failing. Replace the fan FRU.

Severity

WARNING

FW-1008

Message

```
<timestamp>, [FW-1008], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the speed of the fan has changed from a value outside of the acceptable range to a value within the acceptable range. Fan problems typically contribute to temperature problems.

Recommended Action

No action is required. Consistently abnormal fan speeds generally indicate that the fan is failing. If this message occurs repeatedly, replace the fan FRU.

Severity

INFO

FW-1009

Message

```
<timestamp>, [FW-1009], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the state of the power supply has changed from faulty to functional or from functional to faulty.

Recommended Action

If the power supply is functioning correctly, no action is required.

If the power supply is functioning below the acceptable boundary, verify that it is seated correctly in the chassis. Run the **psShow** command to view the status of the power supply. If the power supply continues to be a problem, replace the faulty power supply.

Severity

INFO

FW-1010

Message

```
<timestamp>, [FW-1010], <sequence-number>,, WARNING, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the power supply is faulty. The power supply is not producing enough power.

Recommended Action

Verify that you have installed the power supply correctly and that it is correctly seated in the chassis. If the problem persists, replace the faulty power supply.

Severity

WARNING

FW-1011

Message

```
<timestamp>, [FW-1011], <sequence-number>,, INFO, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the power supply is functioning properly.

Recommended Action

No action is required. Set the high boundary above the normal operation range.

Severity

INFO

FW-1012

Message

```
<timestamp>, [FW-1012], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the power supply counter changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1033

Message

```
<timestamp>, [FW-1033], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the temperature of the SFP has changed.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent fluctuations in SFP temperature might indicate a deteriorating SFP.

Severity

INFO

FW-1034

Message

```
<timestamp>, [FW-1034], <sequence-number>,, WARNING, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the temperature of the SFP has fallen below the low boundary.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

WARNING

FW-1035

Message

```
<timestamp>, [FW-1035], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the temperature of the SFP has risen above the high boundary.

Recommended Action

Frequent fluctuations in temperature might indicate a deteriorating SFP. Replace the SFP.

Severity

WARNING

FW-1036

Message

```
<timestamp>, [FW-1036], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the temperature of the SFP has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action

No action is required.

Frequent fluctuations in temperature might indicate a deteriorating SFP.

Severity

INFO

FW-1037

Message

```
<timestamp>, [FW-1037], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the receive power value of the SFP has changed. The receive performance area measures the amount of incoming laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action

Incoming laser fluctuations usually indicate a deteriorating SFP. If this message occurs repeatedly, replace the SFP.

Severity

INFO

FW-1038

Message

```
<timestamp>, [FW-1038], <sequence-number>,, WARNING, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the receive power value of the SFP has fallen below the low boundary. The receive performance area measures the amount of incoming laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action

Verify that your optical components are clean and function properly. Replace deteriorating cables or SFPs. Check for damage from heat or age.

Severity

WARNING

FW-1039

Message

```
<timestamp>, [FW-1039], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the receive power value of the SFP has risen above the high boundary. The receive performance area measures the amount of incoming laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action

Replace the SFP before it deteriorates.

Severity

WARNING

FW-1040

Message

```
<timestamp>, [FW-1040], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the receive power value of the SFP has changed from a value outside of the acceptable range to a value within the acceptable range. The receive performance area measures the amount of incoming laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1041

Message

```
<timestamp>, [FW-1041], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the transmit power value of the SFP has changed. The transmit performance area measures the amount of outgoing laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action

Transmitting laser fluctuations usually indicate a deteriorating SFP. If this message occurs repeatedly, replace the SFP.

Severity

INFO

FW-1042

Message

```
<timestamp>, [FW-1042], <sequence-number>,, WARNING, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the transmit power value of the SFP has fallen below the low boundary. The transmit performance area measures the amount of outgoing laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action

Verify that your optical components are clean and function properly. Replace deteriorating cables or SFPs. Check for damage from heat or age.

Severity

WARNING

FW-1043

Message

```
<timestamp>, [FW-1043], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the transmit power value of the SFP has risen above the high boundary. The transmit performance area measures the amount of outgoing laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action

Replace the SFP.

Severity

WARNING

FW-1044

Message

```
<timestamp>, [FW-1044], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the transmit power value of the SFP has changed from a value outside of the acceptable range to a value within the acceptable range. The transmit performance area measures the amount of outgoing laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1045

Message

```
<timestamp>, [FW-1045], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the value of the SFP voltage has changed.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. If the supplied voltage of the SFP transceiver is outside of the normal range, this might indicate a hardware failure. Frequent messages indicate that you must replace the SFP.

Severity

INFO

FW-1046

Message

```
<timestamp>, [FW-1046], <sequence-number>,, WARNING, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```


Probable Cause

Indicates that the value of the SFP voltage has fallen below the low boundary.

Recommended Action

Verify that your optical components are clean and function properly. Replace deteriorating cables or SFPs. Check for damage from heat or age.

Severity

WARNING

FW-1047

Message

```
<timestamp>, [FW-1047], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the value of the SFP voltage has risen above the high boundary.

Recommended Action

The supplied current of the SFP transceiver is outside of the normal range, indicating possible hardware failure. If the current rises above the high boundary, you must replace the SFP.

Severity

WARNING

FW-1048

Message

```
<timestamp>, [FW-1048], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the value of the SFP voltage has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1049

Message

```
<timestamp>, [FW-1049], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the value of the SFP voltage has changed.

Recommended Action

Frequent voltage fluctuations are an indication that the SFP is deteriorating. Replace the SFP.

Severity

INFO

FW-1050

Message

```
<timestamp>, [FW-1050], <sequence-number>,, WARNING, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the value of the SFP voltage has fallen below the low boundary.

Recommended Action

Configure the low threshold to 1 so that the threshold triggers an alarm when the value falls to 0 (Out_of_Range). If continuous or repeated alarms occur, replace the SFP before it deteriorates.

Severity

WARNING

FW-1051

Message

```
<timestamp>, [FW-1051], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the value of the SFP voltage has risen above the high boundary. High voltages indicate possible hardware failures.

Recommended Action

Frequent voltage fluctuations are an indication that the SFP is deteriorating. Replace the SFP.

Severity

WARNING

FW-1052

Message

```
<timestamp>, [FW-1052], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the value of the SFP voltage has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1113

Message

```
<timestamp>, [FW-1113], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of times E_Ports have gone down has changed. E_Ports go down each time you remove a cable or SFP. SFP failures also cause E_Ports to go down. E_Port downs might be caused by transient errors.

Recommended Action

Check both ends of the physical connection and verify that the SFPs and cables are functioning properly.

Severity

INFO

FW-1114

Message

```
<timestamp>, [FW-1114], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of times E_Ports have gone down has fallen below the low boundary. E_Ports go down each time you remove a cable or SFP. SFP failures also cause E_Ports to go down. E_Port downs might be caused by transient errors.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of E_Port failures means that the switch is functioning normally.

Severity

INFO

FW-1115

Message

```
<timestamp>, [FW-1115], <sequence-number>,, INFO, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of times E_Ports have gone down has risen above the high boundary. E_Ports go down each time you remove a cable or SFP. SFP failures also cause E_Ports to go down. E_Port downs might be caused by transient errors.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Check both ends of the physical connection and verify that the SFP functions properly.

Severity

INFO

FW-1116

Message

```
<timestamp>, [FW-1116], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of times E_Ports have gone down has changed from a value outside of the acceptable range to a value within the acceptable range. E_Ports go down each time you remove a cable or SFP. SFP failures also cause E_Ports to go down. E_Port downs might be caused by transient errors.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1117

Message

```
<timestamp>, [FW-1117], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of fabric reconfigures has changed. The following actions can cause a fabric reconfiguration:

- two switches with the same domain ID have connected to one another.
- two fabrics have joined.

- an E_Port has gone offline.
- a principal link has segmented from the fabric.

Recommended Action

Verify that the cable is properly connected at both ends. Verify that the SFPs have not become faulty. An inexplicable fabric reconfiguration might be a transient error and might not require troubleshooting.

Severity

INFO

FW-1118

Message

```
<timestamp>, [FW-1118], <sequence-number>,, INFO, <system-name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of fabric reconfigures has fallen below the low boundary. The following occurrences can cause a fabric reconfiguration:

- Two switches with the same domain ID have connected to one another.
- Two fabrics have joined.
- An E_Port has gone offline.
- A principal link has segmented from the fabric.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of fabric reconfigurations means that the fabric is functioning normally.

Severity

INFO

FW-1119

Message

```
<timestamp>, [FW-1119], <sequence-number>,, INFO, <system-name>,
<Label>, is above high boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of fabric reconfigures has risen above the high boundary. The following occurrences can cause a fabric reconfiguration:

- Two switches with the same domain ID have connected to one another.
- Two fabrics have joined.
- An E_Port has gone offline.
- A principal link has segmented from the fabric.

Recommended Action

Verify that all ISL cables are properly connected at both ends. Verify that the SFP has not become faulty. An inexplicable fabric reconfiguration might be a transient error and might not require troubleshooting.

Severity

INFO

FW-1120

Message

```
<timestamp>, [FW-1120], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of fabric reconfigures has changed from a value outside of the acceptable range to a value within the acceptable range. The following occurrences can cause a fabric reconfiguration:

- Two switches with the same domain ID have connected to one another.
- Two fabrics have joined.
- An E_Port has gone offline.
- A principal link has segmented from the fabric.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1121

Message

```
<timestamp>, [FW-1121], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of domain ID changes has changed. Domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch has to assign another domain ID to the switch.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1122

Message

```
<timestamp>, [FW-1122], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of domain ID changes has fallen below the low boundary. Domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch has to assign another domain ID to the switch.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of domain ID changes means that the fabric is functioning normally.

Severity

INFO

FW-1123

Message

```
<timestamp>, [FW-1123], <sequence-number>,, INFO, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of domain ID changes has risen above the high boundary. Domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch has to assign another domain ID to the switch.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1124

Message

```
<timestamp>, [FW-1124], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of domain ID changes has changed from a value outside of the acceptable range to a value within the acceptable range. Domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch has to assign another domain ID to the switch.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1125

Message

```
<timestamp>, [FW-1125], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of segmentations has changed. Segmentation changes might occur due to:

- Zone conflicts.
- Domain conflicts.
- Segmentation of the principal link between two switches.
- Incompatible link parameters. During E_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1126

Message

```
<timestamp>, [FW-1126], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of segmentations has fallen below the low boundary. Segmentation changes might occur due to:

- Zone conflicts.
- Domain conflicts.
- Segmentation of the principal link between two switches.
- Incompatible link parameters. During E_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of segmentation errors means that the fabric is functioning normally.

Severity

INFO

FW-1127

Message

```
<timestamp>, [FW-1127], <sequence-number>,, INFO, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of segmentations has risen above the high boundary. Segmentation changes might occur due to:

- Zone conflicts.
- Domain conflicts.
- Segmentation of the principal link between two switches.
- Incompatible link parameters. During E_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1128

Message

```
<timestamp>, [FW-1128], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of segmentations has changed from a value outside of the acceptable range to a value within the acceptable range. Segmentation changes might occur due to:

- Zone conflicts.
- Domain conflicts.
- Segmentation of the principal link between two switches.
- Incompatible link parameters. During E_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1129

Message

```
<timestamp>, [FW-1129], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of zone changes has changed. Zone changes occur when there is a change to the effective zone configuration.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1130

Message

```
<timestamp>, [FW-1130], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of zone changes has fallen below the low boundary. Zone changes occur when there is a change to the effective zone configuration.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of zone configuration changes means that the fabric is functioning normally.

Severity

INFO

FW-1131

Message

```
<timestamp>, [FW-1131], <sequence-number>,, INFO, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of zone changes has risen above the high boundary. Zone changes occur when there is a change to the effective zone configuration.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1132

Message

```
<timestamp>, [FW-1132], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of zone changes has changed from a value outside of the acceptable range to a value within the acceptable range. Zone changes occur when there is a change to the effective zone configuration.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1133

Message

```
<timestamp>, [FW-1133], <sequence-number>,, INFO, <system-name>, <Label>, value has  
changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of fabric logins has changed. Fabric logins occur when a port or device initializes with the fabric. The event is called a fabric login or FLOGI.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1134

Message

```
<timestamp>, [FW-1134], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of fabric logins has fallen below the low boundary. Fabric logins occur when a port or device initializes with the fabric. The event is called a fabric login or FLOGI.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of fabric logins means that the fabric is functioning normally.

Severity

INFO

FW-1135

Message

```
<timestamp>, [FW-1135], <sequence-number>,, INFO, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of fabric logins has risen above the high boundary. Fabric logins occur when a port or device initializes with the fabric. The event is called a fabric login or FLOGI.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1136

Message

```
<timestamp>, [FW-1136], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of fabric logins has changed from a value outside of the acceptable range to a value within the acceptable range. Fabric logins occur when a port or device initializes with the fabric. The event is called a fabric login or FLOGI.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1137

Message

```
<timestamp>, [FW-1137], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of SFP state changes has changed. SFP state changes occur when the SFP is inserted or removed.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1138

Message

```
<timestamp>, [FW-1138], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of SFP state changes has fallen below the low boundary. SFP state changes occur when the SFP is inserted or removed.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of SFP state changes means that the switch is functioning normally.

Severity

INFO

FW-1139

Message

```
<timestamp>, [FW-1139], <sequence-number>,, INFO, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of SFP state changes has risen above the high boundary. SFP state changes occur when the SFP is inserted or removed.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1140

Message

```
<timestamp>, [FW-1140], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of SFP state changes has changed from a value outside of the acceptable range to a value within the acceptable range. SFP state changes occur when the SFP is inserted or removed.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1160

Message

```
<timestamp>, [FW-1160], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, value has changed(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of link failures that the port experiences has changed. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them.

Recommended Action

Check both ends of your cable connection. Verify that the cable and SFPs are not faulty.

Losses of synchronization commonly causes link failures. If you receive concurrent loss of synchronization errors, troubleshoot the loss of synchronization.

Severity

INFO

FW-1161

Message

```
<timestamp>, [FW-1161], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, is below low boundary(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of link failures that the port experiences has fallen below the low boundary. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems

can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of link loss errors means that the switch is functioning normally.

Severity

INFO

FW-1162

Message

```
<timestamp>, [FW-1162], <sequence-number>,, WARNING, <system-name>,  
<Port Name>, <Label>, is above high boundary(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of link failures that the port experiences has risen above the high boundary. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them.

Recommended Action

Check both ends of your cable connection. Verify that the cable and SFPs are not faulty.

Losses of synchronization commonly cause link failures. If you receive concurrent loss of synchronization errors, troubleshoot the loss of synchronization.

Severity

WARNING

FW-1163

Message

```
<timestamp>, [FW-1163], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, is between high and low boundaries(High=<High  
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of link failures that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1164

Message

```
<timestamp>, [FW-1164], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, value has changed(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of synchronization losses that the port experiences has changed. Loss of synchronization errors frequently occur due to a faulty SFP or cable. Signal losses often create synchronization losses.

Recommended Action

Check both ends of your cable connection. Verify that the cable and SFPs are not faulty.

If you continue to experience synchronization loss errors, troubleshoot your HBA and contact your switch service provider.

Severity

INFO

FW-1165

Message

```
<timestamp>, [FW-1165], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, is below low boundary(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of synchronization losses that the port experiences has fallen below the low boundary. Loss of synchronization errors frequently occur due to a faulty SFP or cable. Signal losses often create synchronization losses.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of synchronization losses means that the switch is functioning normally.

Severity

INFO

FW-1166

Message

```
<timestamp>, [FW-1166], <sequence-number>,, WARNING, <system-name>,  
<Port Name>, <Label>, is above high boundary(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of synchronization losses that the port experiences has risen above the high boundary. Loss-of-synchronization errors frequently occur due to a faulty SFP or cable. Signal losses often create synchronization losses.

Recommended Action

Check both ends of your cable connection. Verify that the cable and SFPs are not faulty.

If you continue to experience loss-of-synchronization errors, troubleshoot your HBA and contact your switch service provider.

Severity

WARNING

FW-1167

Message

```
<timestamp>, [FW-1167], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, is between high and low boundaries (High=<High  
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of synchronization losses that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Loss of synchronization errors frequently occur due to a faulty SFP or cable. Signal losses often create synchronization losses.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1168

Message

```
<timestamp>, [FW-1168], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, value has changed (High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of signal losses that the port experiences has changed. Loss of signal generally indicates a physical problem.

Recommended Action

Check both ends of your cable connection. Verify that the cable and SFPs are not faulty.

Severity

INFO

FW-1169

Message

```
<timestamp>, [FW-1169], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, is below low boundary (High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of signal losses that the port experiences has fallen below the low boundary. Loss of signal generally indicates a physical problem.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of signal loss errors means that the switch is functioning normally.

Severity

INFO

FW-1170

Message

```
<timestamp>, [FW-1170], <sequence-number>,, WARNING, <system-name>,  
<Port Name>, <Label>, is above high boundary(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of signal losses that the port experiences has risen above the high boundary. Loss of signal generally indicates a physical problem.

Recommended Action

Check both ends of your cable connection. Verify that the cable is not faulty.

Severity

WARNING

FW-1171

Message

```
<timestamp>, [FW-1171], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, is between high and low boundaries(High=<High  
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of signal losses that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Loss of signal generally indicates a physical problem.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent loss of signal generally indicates a physical problem.

Check both ends of your cable connection. Verify that the cable and SFPs are not faulty.

Severity

INFO

FW-1172

Message

```
<timestamp>, [FW-1172], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, value has changed(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of protocol errors that the port experiences has changed. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems.

Recommended Action

Check both ends of your cable connection. Verify that the cable and SFPs are not faulty.

Severity

INFO

FW-1173

Message

```
<timestamp>, [FW-1173], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, is below low boundary(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of protocol errors that the port experiences has fallen below the low boundary. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of protocol errors means that the switch is functioning normally.

Severity

INFO

FW-1174

Message

```
<timestamp>, [FW-1174], <sequence-number>,, WARNING, <system-name>,  
<Port Name>, <Label>, is above high boundary(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of protocol errors that the port experiences has risen above the high boundary. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems.

Recommended Action

Check both ends of your connection. Verify that your cable and SFP are not faulty.

Severity

WARNING

FW-1175

Message

```
<timestamp>, [FW-1175], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, is between high and low boundaries (High=<High  
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of protocol errors that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1176

Message

```
<timestamp>, [FW-1176], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, value has changed (High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of invalid words that the port experiences has changed. Invalid words usually indicate a hardware problem with an SFP or cable.

Recommended Action

Check both ends of your connections, your SFP, and your cable to verify that none are faulty.

Severity

INFO

FW-1177

Message

```
<timestamp>, [FW-1177], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, is below low boundary (High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of invalid words that the port experiences has fallen below the low boundary. Invalid words usually indicate a hardware problem with an SFP or cable.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of invalid words means that the switch is functioning normally.

Severity

INFO

FW-1178

Message

```
<timestamp>, [FW-1178], <sequence-number>,, WARNING, <system-name>,  
<Port Name>, <Label>, is above high boundary(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of invalid words that the port experiences has risen above the high boundary. Invalid words usually indicate a hardware problem with an SFP or cable.

Recommended Action

Check both ends of your connections, your SFP, and your cable to verify that none are faulty.

Severity

WARNING

FW-1179

Message

```
<timestamp>, [FW-1179], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, is between high and low boundaries(High=<High  
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of invalid words that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Invalid words usually indicate a hardware problem with an SFP or cable.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1180

Message

```
<timestamp>, [FW-1180], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, value has changed(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of invalid CRCs that the port experiences has changed.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent fluctuations in CRC errors generally indicate an aging fabric. Check your SFPs, cables, and connections for faulty hardware. Verify that all optical hardware is clean.

Severity

INFO

FW-1181

Message

```
<timestamp>, [FW-1181], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, is below low boundary(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of invalid CRCs that the port experiences has fallen below the low boundary.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of invalid CRCs means that the switch is functioning normally.

Severity

INFO

FW-1182

Message

```
<timestamp>, [FW-1182], <sequence-number>,, WARNING, <system-name>,  
<Port Name>, <Label>, is above high boundary(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of invalid CRCs that the port experiences has risen above the high boundary.

Recommended Action

This error generally indicates an deteriorating fabric hardware. Check your SFPs, cables, and connections for faulty hardware. Verify that all optical hardware is clean.

Severity

WARNING

FW-1183

Message

```
<timestamp>, [FW-1183], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, is between high and low boundaries(High=<High  
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of invalid CRCs that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent fluctuations in CRC errors generally indicate an aging fabric. Check your SFPs, cables, and connections for faulty hardware. Verify that all optical hardware is clean.

Severity

INFO

FW-1184

Message

```
<timestamp>, [FW-1184], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, value has changed(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the percentage of incoming traffic that the port experiences has changed.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1185

Message

```
<timestamp>, [FW-1185], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, is below low boundary(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the percentage of incoming traffic that the port experiences has fallen below the low boundary.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1186

Message

```
<timestamp>, [FW-1186], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, is above high boundary(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the percentage of incoming traffic that the port experiences has risen above the high boundary.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1187

Message

```
<timestamp>, [FW-1187], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, is between high and low boundaries(High=<High  
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the percentage of incoming traffic that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1188

Message

```
<timestamp>, [FW-1188], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, value has changed(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the percentage of outgoing traffic that the port experiences has changed.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1189

Message

```
<timestamp>, [FW-1189], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, is below low boundary(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the percentage of outgoing traffic that the port experiences has fallen below the low boundary.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1190

Message

```
<timestamp>, [FW-1190], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, is above high boundary(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the percentage of outgoing traffic that the port experiences has risen above the high boundary.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1191

Message

```
<timestamp>, [FW-1191], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, is between high and low boundaries(High=<High  
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the percentage of outgoing traffic that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1192

Message

```
<timestamp>, [FW-1192], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, value has changed(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of state changes that the port experiences has changed. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E_Port, has become an F_Port, has segmented, or has become a trunk port.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1193

Message

```
<timestamp>, [FW-1193], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, is below low boundary(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of state changes that the port experiences has fallen below the low boundary. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E_Port, has become an F_Port, has segmented, or has become a trunk port.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of port state changes means that the switch is functioning normally.

Severity

INFO

FW-1194

Message

```
<timestamp>, [FW-1194], <sequence-number>,, WARNING, <system-name>,  
<Port Name>, <Label>, is above high boundary(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of state changes that the port experiences has risen above the high boundary. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E_Port, has become an F_Port, has segmented, or has become a trunk port.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

WARNING

FW-1195

Message

```
<timestamp>, [FW-1195], <sequence-number>,, INFO, <system-name>,  
<Port Name>, <Label>, is between high and low boundaries(High=<High  
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of state changes that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E_Port, has become an F_Port, has segmented, or has become a trunk port.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1216

Message

```
<timestamp>, [FW-1216], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of AL_PA CRC errors has changed. This indicates that errors have been detected in the FC frame. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by

dirty equipment, temperature fluctuations, and aging equipment. You should set your high boundaries to five- or six-digit figures, as only large numbers of messages indicate a problem in this area.

Recommended Action

Verify that your optical components are clean and function properly. Replace deteriorating cables or SFPs. Check for damage from heat or age.

Severity

INFO

FW-1217

Message

```
<timestamp>, [FW-1217], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of AL_PA CRC errors has fallen below the low boundary. This indicates that errors have been detected in the FC frame. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment. You should set your high boundaries to five- or six-digit figures, as only large numbers of messages indicate a problem in this area.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low level of invalid CRC errors means that the switch is functioning normally.

Severity

INFO

FW-1218

Message

```
<timestamp>, [FW-1218], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of CRC errors has risen above the high boundary. This indicates that errors have been detected in the FC frame. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment. You should set your high boundaries to five- or six-digit figures, as only large numbers of messages indicate a problem in this area.

Recommended Action

You should configure a five- or six-figure high boundary for this area. Only five-figure (or higher) values for CRC errors indicate problems. When an "above" message is received, check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary. Try cleaning the connectors. Check for damage from heat or deterioration from age.

Severity

WARNING

FW-1219

Message

```
<timestamp>, [FW-1219], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of CRC errors has changed from a value outside of the acceptable range to a value within the acceptable range. This indicates that errors have been detected in the FC frame. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment. You should set your high boundaries to five- or six-digit figures, as only large numbers of messages indicate a problem in this area.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1240

Message

```
<timestamp>, [FW-1240], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of EE CRC errors has changed. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1241

Message

```
<timestamp>, [FW-1241], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of EE CRC errors has fallen below the low boundary. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of CRC errors means that the fabric is functioning normally. The CRC error area of the End-to-End Performance Monitor class helps you tune your fabric. To reduce CRC messages, experiment with alternative topologies and cabling schemes.

Severity

INFO

FW-1242

Message

```
<timestamp>, [FW-1242], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of EE CRC errors has risen above the high boundary. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment.

Recommended Action

The CRC error area of the End-to-End Performance Monitor class helps the user tune the fabric. To reduce CRC errors, experiment with alternative topologies and cabling schemes. Clean equipment, check temperatures, and replace old hardware.

Severity

WARNING

FW-1243

Message

```
<timestamp>, [FW-1243], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of EE CRC errors has changed from a value outside of the acceptable range to a value within the acceptable range. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1244

Message

```
<timestamp>, [FW-1244], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of EE word frames that the switch receives has changed. Receive performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1245

Message

```
<timestamp>, [FW-1245], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of EE word frames that the switch receives has fallen below the low boundary. Receive performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1246

Message

```
<timestamp>, [FW-1246], <sequence-number>,, INFO, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of EE word frames that the switch receives has risen above the high boundary. Receive performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1247

Message

```
<timestamp>, [FW-1247], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of EE word frames that the switch receives has changed from a value outside of the acceptable range to a value within the acceptable range. Receive performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1248

Message

```
<timestamp>, [FW-1248], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of EE word frames that the switch transmits has changed. Transmit performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1249

Message

```
<timestamp>, [FW-1249], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```


Probable Cause

Indicates that the number of EE word frames that the switch transmits has fallen below the low boundary. Transmit performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1250

Message

```
<timestamp>, [FW-1250], <sequence-number>,, INFO, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of EE word frames that the switch transmits has risen above the high boundary. Transmit performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1251

Message

```
<timestamp>, [FW-1251], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of EE word frames that the switch transmits has changed from a value outside of the acceptable range to a value within the acceptable range. Transmit performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1272

Message

```
<timestamp>, [FW-1272], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of frame types or commands that the port receives has changed. The port has received SCSI Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1273

Message

```
<timestamp>, [FW-1273], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of frame types or commands that the port receives has fallen below the low boundary. The port has received SCSI Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1274

Message

```
<timestamp>, [FW-1274], <sequence-number>,, INFO, <system-name>,  
<Label>, is above high boundary(High=<Filter Counter>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of frame types or commands that the port receives has risen above the high boundary. The port has received SCSI Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1275

Message

```
<timestamp>, [FW-1275], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of frame types or commands that the port receives has changed from a value outside of the acceptable range to a value within the acceptable range. The port has received SCSI Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1296

Message

```
<timestamp>, [FW-1296], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of telnet violations has changed. Telnet violations indicate that a telnet connection request has been received from an unauthorized IP address. The TELNET_POLICY contains a list of TCP/IP addresses that are authorized to establish telnet connections to switches in the fabric. The IP addresses use standard "dot" notation (for example, 255.255.255.255).

Recommended Action

Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1297

Message

```
<timestamp>, [FW-1297], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of telnet violations has fallen below the low boundary. Telnet violations indicate that a telnet connection request has been received from an unauthorized IP address. The TELNET_POLICY contains a list of TCP/IP addresses that are authorized to establish telnet connections to switches in the fabric. The IP addresses use standard "dot" notation (for example, 255.255.255.255).

Recommended Action

No action is required.

Severity

INFO

FW-1298

Message

```
<timestamp>, [FW-1298], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of telnet violations has risen above the high boundary. Telnet violations indicate that a telnet connection request has been received from an unauthorized IP address. The TELNET_POLICY contains a list of TCP/IP addresses that are authorized to establish telnet connections to switches in the fabric. The IP addresses use standard "dot" notation (for example, 255.255.255.255).

Recommended Action

Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1299

Message

```
<timestamp>, [FW-1299], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of telnet violations has changed from a value outside of the acceptable range to a value within the acceptable range. Telnet violations indicate that a telnet connection request has been received from an unauthorized IP address. The TELNET_POLICY contains a list of TCP/IP addresses that are

authorized to establish telnet connections to switches in the fabric. The IP addresses use standard "dot" notation (for example, 255.255.255.255).

Recommended Action

No action is required.

Severity

INFO

FW-1300

Message

```
<timestamp>, [FW-1300], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of HTTP violations has changed. HTTP violations indicate that a browser connection request has been received from an unauthorized IP address. The HTTP_POLICY contains a list of TCP/IP addresses that are authorized to establish browser connections to the switches in the fabric. The IP addresses use the standard "dot" notation (for example, 255.255.255.255).

Recommended Action

Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1301

Message

```
<timestamp>, [FW-1301], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of HTTP violations has fallen below the low boundary. HTTP violations indicate that a browser connection request has been received from an unauthorized IP address. The HTTP_POLICY contains a list of TCP/IP addresses that are authorized to establish browser connections to the switches in the fabric. The IP addresses use the standard "dot" notation (for example, 255.255.255.255).

Recommended Action

No action is required.

Severity

INFO

FW-1302

Message

```
<timestamp>, [FW-1302], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of HTTP violations has risen above the high boundary. HTTP violations indicate that a browser connection request has been received from an unauthorized IP address. The HTTP_POLICY contains a list of TCP/IP addresses that are authorized to establish browser connections to the switches in the fabric. The IP addresses use the standard "dot" notation (for example, 255.255.255.255).

Recommended Action

Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1303

Message

```
<timestamp>, [FW-1303], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of HTTP violations has changed from a value outside of the acceptable range to a value within the acceptable range. HTTP violations indicate that a browser connection request has been received from an unauthorized IP address. The HTTP_POLICY contains a list of TCP/IP addresses that are authorized to establish browser connections to the switches in the fabric. The IP addresses use the standard "dot" notation (for example, 255.255.255.255).

Recommended Action

No action is required.

Severity

INFO

FW-1304

Message

```
<timestamp>, [FW-1304], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of API violations has changed. API violations indicate that an API connection request has been received from an unauthorized IP address. The SNMP_POLICY contains a list of TCP/IP

addresses that are authorized to establish API connections to switches in the fabric. The IP addresses use standard "dot" notation (for example, 255.255.255.255).

Recommended Action

Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1305

Message

```
<timestamp>, [FW-1305], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of API violations has fallen below the low boundary. API violations indicate that an API connection request has been received from an unauthorized IP address. The SNMP_POLICY contains a list of TCP/IP addresses that are authorized to establish API connections to switches in the fabric. The IP addresses use standard "dot" notation (for example, 255.255.255.255).

Recommended Action

No action is required.

Severity

INFO

FW-1306

Message

```
<timestamp>, [FW-1306], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of API violations has risen above the high boundary. API violations indicate that an API connection request has been received from an unauthorized IP address. The SNMP_POLICY contains a list of TCP/IP addresses that are authorized to establish API connections to switches in the fabric. The IP addresses use standard "dot" notation (for example, 255.255.255.255).

Recommended Action

Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1307

Message

```
<timestamp>, [FW-1307], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of API violations has changed from a value outside of the acceptable range to a value within the acceptable range. API violations indicate that an API connection request has been received from an unauthorized IP address. The SNMP_POLICY contains a list of TCP/IP addresses that are authorized to establish API connections to switches in the fabric. The IP addresses use standard "dot" notation (for example, 255.255.255.255).

Recommended Action

No action is required.

Severity

INFO

FW-1308

Message

```
<timestamp>, [FW-1308], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of RSNMP violations has changed. RSNMP violations indicate that an SNMP "get" operation request has been received from an unauthorized IP address.

Recommended Action

Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1309

Message

```
<timestamp>, [FW-1309], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of RSNMP violations has fallen below the low boundary. RSNMP violations indicate that an SNMP "get" operation request has been received from an unauthorized IP address.

Recommended Action

No action is required.

Severity

INFO

FW-1310

Message

```
<timestamp>, [FW-1310], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of RSNMP violations has risen above the high boundary. RSNMP violations indicate that an SNMP "get" operation request has been received from an unauthorized IP address.

Recommended Action

Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1311

Message

```
<timestamp>, [FW-1311], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of RSNMP violations has changed from a value outside of the acceptable range to a value within the acceptable range. RSNMP violations indicate that an SNMP "get" operation request has been received from an unauthorized IP address.

Recommended Action

No action is required.

Severity

INFO

FW-1312

Message

```
<timestamp>, [FW-1312], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of WSNMP violations has changed. WSNMP violations indicate that an SNMP "get/set" operation request has been received from an unauthorized IP address.

Recommended Action

Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1313

Message

```
<timestamp>, [FW-1313], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of WSNMP violations has fallen below the low boundary. WSNMP violations indicate that an SNMP "get/set" operation request has been received from an unauthorized IP address.

Recommended Action

No action is required.

Severity

INFO

FW-1314

Message

```
<timestamp>, [FW-1314], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of WSNMP violations has risen above the high boundary. WSNMP violations indicate that an SNMP "get/set" operation request has been received from an unauthorized IP address.

Recommended Action

Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1315

Message

```
<timestamp>, [FW-1315], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of WSNMP violations has changed from a value outside of the acceptable range to a value within the acceptable range. WSNMP violations indicate that an SNMP "get/set" operation request has been received from an unauthorized IP address.

Recommended Action

No action is required.

Severity

INFO

FW-1316

Message

```
<timestamp>, [FW-1316], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of SES violations has changed. SES violations indicate that an SCSI Enclosure Services (SES) request has been received from an unauthorized WWN. The SES_POLICY contains a list of WWNs of device ports that are allowed to access the SES Server functionality.

Recommended Action

Run the **errShow** command to determine the IP address that sent the request. Responses to security class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1317

Message

```
<timestamp>, [FW-1317], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of SES violations has fallen below the low boundary. SES violations indicate that an SCSI Enclosure Services (SES) request has been received from an unauthorized WWN. The SES_POLICY contains a list of WWNs of device ports that are allowed to access the SES Server functionality.

Recommended Action

No action is required.

Severity

INFO

FW-1318

Message

```
<timestamp>, [FW-1318], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of SES violations has risen above the high boundary. SES violations indicate that an SCSI Enclosure Services (SES) request has been received from an unauthorized WWN. The SES_POLICY contains a list of WWNs of device ports that are allowed to access the SES Server functionality.

Recommended Action

Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1319

Message

```
<timestamp>, [FW-1319], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of SES violations has changed from a value outside of the acceptable range to a value within the acceptable range. SES violations indicate that an SCSI Enclosure Services (SES) request has been received from an unauthorized WWN. The SES_POLICY contains a list of WWNs of device ports that are allowed to access the SES Server functionality.

Recommended Action

No action is required.

Severity

INFO

FW-1320

Message

```
<timestamp>, [FW-1320], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of MS violations has changed. MS violations indicate that a Management Server (MS) access request has been received from an unauthorized WWN. The MS_POLICY contains a list of WWNs of device ports that are allowed to access the Management Server functionality.

Recommended Action

Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1321

Message

```
<timestamp>, [FW-1321], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of MS violations has fallen below the low boundary. MS violations indicate that a Management Server (MS) access request has been received from an unauthorized WWN. The MS_POLICY contains a list of WWNs of device ports that are allowed to access the Management Server functionality.

Recommended Action

No action is required.

Severity

INFO

FW-1322

Message

```
<timestamp>, [FW-1322], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of MS violations has risen above the high boundary. MS violations indicate that a Management Server (MS) access request has been received from an unauthorized WWN. The MS_POLICY contains a list of WWNs of device ports that are allowed to access the Management Server functionality.

Recommended Action

Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1323

Message

```
<timestamp>, [FW-1323], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of MS violations has changed from a value outside of the acceptable range to a value within the acceptable range. MS violations indicate that a Management Server (MS) access request has been received from an unauthorized WWN. The MS_POLICY contains a list of WWNs of device ports that are allowed to access the Management Server functionality.

Recommended Action

No action is required.

Severity

INFO

FW-1324

Message

```
<timestamp>, [FW-1324], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of serial violations has changed. Serial violations indicate that an unauthorized serial port request has been received. The SERIAL_POLICY contains a list of switch WWNs for which serial port access is enabled.

Recommended Action

Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1325

Message

```
<timestamp>, [FW-1325], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of serial violations has fallen below the low boundary. Serial violations indicate that an unauthorized serial port request has been received. The SERIAL_POLICY contains a list of switch WWNs for which serial port access is enabled.

Recommended Action

No action is required.

Severity

INFO

FW-1326

Message

```
<timestamp>, [FW-1326], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of serial violations has risen above the high boundary. Serial violations indicate that an unauthorized serial port request has been received. The SERIAL_POLICY contains a list of switch WWNs for which serial port access is enabled.

Recommended Action

Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1327

Message

```
<timestamp>, [FW-1327], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of serial violations has changed from a value outside of the acceptable range to a value within the acceptable range. Serial violations indicate that an unauthorized serial port request has been received. The SERIAL_POLICY contains a list of switch WWNs for which serial port access is enabled.

Recommended Action

No action is required.

Severity

INFO

FW-1328

Message

```
<timestamp>, [FW-1328], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of front panel violations has changed. Front panel violations indicate that an unauthorized front panel request has been received. The FRONT_PANEL_POLICY contains a list of switch WWNs for which front panel access is enabled.

Recommended Action

Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1329

Message

```
<timestamp>, [FW-1329], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of front panel violations has fallen below the low boundary. Front panel violations indicate that an unauthorized front panel request has been received. The FRONT_PANEL_POLICY contains a list of switch WWNs for which front panel access is enabled.

Recommended Action

No action is required.

Severity

INFO

FW-1330

Message

```
<timestamp>, [FW-1330], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of front panel violations has risen above the high boundary. Front panel violations indicate that an unauthorized front panel request has been received. The FRONT_PANEL_POLICY contains a list of switch WWNs for which front panel access is enabled.

Recommended Action

Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1331

Message

```
<timestamp>, [FW-1331], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of front panel violations has changed from a value outside of the acceptable range to a value within the acceptable range. Front panel violations indicate that an unauthorized front panel request has been received. The FRONT_PANEL_POLICY contains a list of switch WWNs for which front panel access is enabled.

Recommended Action

No action is required.

Severity

INFO

FW-1332

Message

```
<timestamp>, [FW-1332], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of SCC violations has changed. SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC_POLICY contains a list of switches by WWN that are allowed to be members of a fabric.

Recommended Action

Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1333

Message

```
<timestamp>, [FW-1333], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of SCC violations has fallen below the low boundary. SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC_POLICY contains a list of switches by WWN that are allowed to be members of a fabric.

Recommended Action

No action is required.

Severity

INFO

FW-1334

Message

```
<timestamp>, [FW-1334], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of SCC violations has risen above the high boundary. SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC_POLICY contains a list of switches by WWN that are allowed to be members of a fabric.

Recommended Action

Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1335

Message

```
<timestamp>, [FW-1335], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of SCC violations has changed from a value outside of the acceptable range to a value within the acceptable range. SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC_POLICY contains a list of switches by WWN that are allowed to be members of a fabric.

Recommended Action

No action is required.

Severity

INFO

FW-1336

Message

```
<timestamp>, [FW-1336], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of DCC violations has changed. DCC violations indicate that an unauthorized device tried to join the fabric. The DCC_POLICY allows for the specification of rules for binding device ports (typically HBA ports) to specific switch ports. DCC policies ensure that whenever a device performs an FLOGI request, the WWN specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the name server.

Recommended Action

Run the **errShow** command to determine the device WWN, switch WWN, and switch port. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1337

Message

```
<timestamp>, [FW-1337], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of DCC violations has fallen below the low boundary. DCC violations indicate that an unauthorized device tried to join the fabric. The DCC_POLICY allows for the specification of rules for binding device ports (typically HBA ports) to specific switch ports. DCC policies ensure that whenever a device performs an FLOGI request, the WWN specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the name server.

Recommended Action

No action is required.

Severity

INFO

FW-1338

Message

```
<timestamp>, [FW-1338], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of DCC violations has risen above the high boundary. DCC violations indicate that an unauthorized device tried to join the fabric. The DCC_POLICY allows for the specification of rules for binding device ports (typically HBA ports) to specific switch ports. DCC policies ensure that whenever a device performs an FLOGI request that the WWN specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the name server.

Recommended Action

Run the **errShow** command to determine the device WWN, switch WWN, and switch port. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1339

Message

```
<timestamp>, [FW-1339], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of DCC violations has changed from a value outside of the acceptable range to a value within the acceptable range. DCC violations indicate that an unauthorized device tried to join the fabric. The DCC_POLICY allows for the specification of rules for binding device ports (typically HBA ports) to specific switch ports. DCC policies ensure that whenever a device performs an FLOGI request that the WWN specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the name server.

Recommended Action

No action is required.

Severity

INFO

FW-1340

Message

```
<timestamp>, [FW-1340], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of login violations has changed. Login violations indicate that a login failure has been detected.

Recommended Action

Run the **errShow** command to determine the IP location of the login attempt. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1341

Message

```
<timestamp>, [FW-1341], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of login violations has fallen below the low boundary. Login violations indicate that a login failure has been detected.

Recommended Action

No action is required.

Severity

INFO

FW-1342

Message

```
<timestamp>, [FW-1342], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of login violations has risen above the high boundary. Login violations indicate that a login failure has been detected.

Recommended Action

Run the **errShow** command to determine the IP location of the login attempt. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1343

Message

```
<timestamp>, [FW-1343], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of login violations has changed from a value outside of the acceptable range to a value within the acceptable range. Login violations indicate that a login failure has been detected.

Recommended Action

No action is required.

Severity

INFO

FW-1344

Message

```
<timestamp>, [FW-1344], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of invalid timestamps has changed. Invalid-timestamp violations indicate that a packet with an invalid timestamp has been received from the primary FCS. When the primary fabric configuration server (FCS) downloads a new configuration to other switches in the fabric, the packet is tagged with a timestamp. The receiving switch compares this timestamp to its current time. If the difference is too great, it rejects the packet. This counter keeps track of packets rejected due to invalid timestamps.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1345

Message

```
<timestamp>, [FW-1345], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of invalid timestamps has fallen below the low boundary. Invalid-timestamp violations indicate a packet with an invalid timestamp has been received from the primary FCS. When the primary fabric configuration server (FCS) downloads a new configuration to other switches in the fabric, the packet is tagged with a timestamp. The receiving switch compares this timestamp to its current time. If the difference is too great, it rejects the packet. This counter keeps track of packets rejected due to invalid timestamps.

Recommended Action

No action is required.

Severity

INFO

FW-1346

Message

```
<timestamp>, [FW-1346], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of invalid timestamps has risen above the high boundary. Invalid-timestamp violations indicate a packet with an invalid timestamp has been received from the primary FCS. When the primary fabric configuration server (FCS) downloads a new configuration to other switches in the fabric, the packet is tagged with a timestamp. The receiving switch compares this timestamp to its current time. If the difference is too great, it rejects the packet. This counter keeps track of packets rejected due to invalid timestamps.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1347

Message

```
<timestamp>, [FW-1347], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of invalid timestamps has changed from a value outside of the acceptable range to a value within the acceptable range. Invalid-timestamp violations indicate a packet with an invalid timestamp has been received from the primary FCS. When the primary fabric configuration server (FCS) downloads a new configuration to other switches in the fabric, the packet is tagged with a timestamp. The receiving switch compares this timestamp to its current time. If the difference is too great, it rejects the packet. This counter keeps track of packets rejected due to invalid timestamps.

Recommended Action

No action is required.

Severity

INFO

FW-1348

Message

```
<timestamp>, [FW-1348], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of invalid signatures has changed. Invalid-signature violations indicate that a packet with an invalid signature has been received from the primary FCS. When the primary fabric configuration server (FCS) downloads a new configuration to the other switches in the fabric, the packet is signed using the private key of the primary FCS. The receiving switch has to verify this signature with the public key of the primary FCS switch. If verification fails, it rejects the packet. This counter keeps track of the number of packets received with invalid signatures.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1349

Message

```
<timestamp>, [FW-1349], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of invalid signatures has fallen below the low boundary. Invalid-signature violations indicate that a packet with an invalid signature has been received from the primary FCS. When the primary fabric configuration server (FCS) downloads a new configuration to the other switches in the fabric, the packet is signed using the private key of the primary FCS. The receiving switch has to verify this signature with the public key of the primary FCS switch. If verification fails, it rejects the packet. This counter keeps track of the number of packets received with invalid signatures.

Recommended Action

No action is required.

Severity

INFO

FW-1350

Message

```
<timestamp>, [FW-1350], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of invalid signatures has risen above the high boundary. Invalid-signature violations indicate that a packet with an invalid signature has been received from the primary FCS. When the primary fabric configuration server (FCS) downloads a new configuration to the other switches in the fabric, the packet is signed using the private key of the primary FCS. The receiving switch has to verify this signature with the public key of the primary FCS switch. If verification fails, it rejects the packet. This counter keeps track of the number of packets received with invalid signatures.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1351

Message

```
<timestamp>, [FW-1351], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of invalid signatures has changed from a value outside of the acceptable range to a value within the acceptable range. Invalid-signature violations indicate that a packet with an invalid signature has been received from the primary FCS. When the primary fabric configuration server (FCS) downloads a new configuration to the other switches in the fabric, the packet is signed using the private key of the primary FCS. The receiving switch has to verify this signature with the public key of the primary FCS switch. If verification fails, it rejects the packet. This counter keeps track of the number of packets received with invalid signatures.

Recommended Action

No action is required.

Severity

INFO

FW-1352

Message

```
<timestamp>, [FW-1352], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of invalid certificates has changed. This violation indicates that a packet with an invalid certificate has been received from the primary FCS. Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch has to verify that the sender is the primary FCS switch and its certificate is signed by the Root CA recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1353

Message

```
<timestamp>, [FW-1353], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of invalid certificates has fallen below the low boundary. This violation indicates that a packet with an invalid certificate has been received from the primary FCS. Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch has to verify that the sender is the primary FCS switch and its certificate is signed by the Root CA recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

Recommended Action

No action is required.

Severity

INFO

FW-1354

Message

```
<timestamp>, [FW-1354], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of invalid certificates has risen above the high boundary. This violation indicates that a packet with an invalid certificate has been received from the primary FCS. Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch has to verify that the sender is the primary FCS switch and its certificate is signed by the Root CA recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1355

Message

```
<timestamp>, [FW-1355], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of invalid certificates has changed from a value outside of the acceptable range to a value within the acceptable range. This violation indicates that a packet with an invalid certificate has been received from the primary FCS. Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch has to verify that the sender is the primary FCS switch and its certificate is signed by the Root CA recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

Recommended Action

No action is required.

Severity

INFO

FW-1356

Message

```
<timestamp>, [FW-1356], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of authentication failures has changed. Authentication failures can occur for many reasons. The switch on the other side might not support the protocol, have an invalid certificate, not be signed properly, or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1357

Message

```
<timestamp>, [FW-1357], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of authentication failures has fallen below the low boundary. Authentication failures can occur for many reasons. The switch on the other side might not support the protocol, have an invalid certificate, not be signed properly or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

Recommended Action

No action is required.

Severity

INFO

FW-1358

Message

```
<timestamp>, [FW-1358], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of authentication failures has risen above the high boundary. Authentication failures can occur for many reasons. The switch on the other side might not support the protocol, have an invalid certificate, not be signed properly or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1359

Message

```
<timestamp>, [FW-1359], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of authentication failures has changed from a value outside of the acceptable range to a value within the acceptable range. Authentication failures can occur for many reasons. The switch on the other side might not support the protocol, have an invalid certificate, not be signed properly or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

Recommended Action

No action is required.

Severity

INFO

FW-1360

Message

```
<timestamp>, [FW-1360], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of SLAP faulty packets has changed. This counter keeps track of the number of unexpected SLAP packets and SLAP packets with faulty transmission IDs.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1361

Message

```
<timestamp>, [FW-1361], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of SLAP faulty packets has fallen below the low boundary. This counter keeps track of the number of unexpected SLAP packets and SLAP packets with faulty transmission IDs.

Recommended Action

No action is required.

Severity

INFO

FW-1362

Message

```
<timestamp>, [FW-1362], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of SLAP faulty packets has risen above the high boundary. This counter keeps track of the number of unexpected SLAP packets and SLAP packets with faulty transmission IDs.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1363

Message

```
<timestamp>, [FW-1363], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of SLAP faulty packets has changed from a value outside of the acceptable range to a value within the acceptable range. This counter keeps track of the number of unexpected SLAP packets and SLAP packets with faulty transmission IDs.

Recommended Action

No action is required.

Severity

INFO

FW-1364

Message

```
<timestamp>, [FW-1364], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of time service (TS) out-of-sync violations has changed.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1365

Message

```
<timestamp>, [FW-1365], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of time service out-of-sync violations has fallen below the low boundary.

Recommended Action

No action is required.

Severity

INFO

FW-1366

Message

```
<timestamp>, [FW-1366], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of time service (TS) out-of-sync violations has risen above the high boundary.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1367

Message

```
<timestamp>, [FW-1367], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of time service (TS) out-of-sync violations has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action

No action is required.

Severity

INFO

FW-1368

Message

```
<timestamp>, [FW-1368], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of no-FCS violations has changed. This counter records how often the switch loses contact with the primary FCS switch. When the primary FCS switch in the fabric sends its certificate to a switch, the receiving switch saves the WWN of that primary FCS switch. If a secure switch finds that there are no FCSs in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1369

Message

```
<timestamp>, [FW-1369], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of no-FCS violations has fallen below the low boundary. This counter records how often the switch loses contact with the primary FCS switch. When the primary FCS switch in the fabric

sends its certificate to a switch, the receiving switch saves the WWN of that primary FCS switch. If a secure switch finds that there are no FCSs in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

Recommended Action

No action is required.

Severity

INFO

FW-1370

Message

```
<timestamp>, [FW-1370], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of no-FCS violations has risen above the high boundary. This counter records how often the switch loses contact with the primary FCS switch. When the primary FCS switch in the fabric sends its certificate to a switch, the receiving switch saves the WWN of that primary FCS switch. If a secure switch finds that there are no FCSs in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1371

Message

```
<timestamp>, [FW-1371], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of no-FCS violations has changed from a value outside of the acceptable range to a value within the acceptable range. This counter records how often the switch loses contact with the primary FCS switch. When the primary FCS switch in the fabric sends its certificate to a switch, the receiving switch saves the WWN of that primary FCS switch. If a secure switch finds that there are no FCSs in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

Recommended Action

No action is required.

Severity

INFO

FW-1372

Message

```
<timestamp>, [FW-1372], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of incompatible security database violations has changed. This violation indicates the number of secure switches with different version stamps have been detected. When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and FCS policy matches exactly.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1373

Message

```
<timestamp>, [FW-1373], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of incompatible security database violations has fallen below the low boundary. This violation indicates the number of secure switches with different version stamps have been detected. When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and FCS policy matches exactly.

Recommended Action

No action is required.

Severity

INFO

FW-1374

Message

```
<timestamp>, [FW-1374], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of incompatible security database violations has risen above the high boundary. This violation indicates the number of secure switches with different version stamps have been detected. When a switch is in secure mode, it connects only to another switch that is in secure mode and has a

compatible security database. A compatible security database means that the version stamp and FCS policy matches exactly.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1375

Message

```
<timestamp>, [FW-1375], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of incompatible security database violations has changed from a value outside of the acceptable range to a value within the acceptable range. This violation indicates the number of secure switches with different version stamps have been detected. When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and FCS policy matches exactly.

Recommended Action

No action is required.

Severity

INFO

FW-1376

Message

```
<timestamp>, [FW-1376], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of illegal commands has changed. This counter tracks how many times commands allowed only on the primary FCS switch have been executed on a non-primary FCS switch. There are many commands that can be executed only on the primary FCS switch as well as one security command that can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1377

Message

```
<timestamp>, [FW-1377], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of illegal commands has fallen below the low boundary. This counter tracks how many times commands allowed only on the primary FCS switch have been executed on a non-primary FCS switch. There are many commands that can be executed only on the primary FCS switch as well as one security command that can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

Recommended Action

No action is required.

Severity

INFO

FW-1378

Message

```
<timestamp>, [FW-1378], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of illegal commands has risen above the high boundary. This counter tracks how many times commands allowed only on the primary FCS switch have been executed on a non-primary FCS switch. There are many commands that can be executed only on the primary FCS switch as well as one security command that can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1379

Message

```
<timestamp>, [FW-1379], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of illegal commands has changed from a value outside of the acceptable range to a value within the acceptable range. This counter tracks how many times commands allowed only on the

primary FCS switch have been executed on a non-primary FCS switch. There are many commands that can be executed only on the primary FCS switch as well as one security command that can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

Recommended Action

No action is required.

Severity

INFO

FW-1400

Message

```
<timestamp>, [FW-1400], <sequence-number>,, INFO, <system-name>,  
<Label>, value has changed(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the flash usage percentage has changed. Flash increases and decreases slightly with normal operation of the switch. Excessive permanent increases can lead to future problems.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1401

Message

```
<timestamp>, [FW-1401], <sequence-number>,, INFO, <system-name>,  
<Label>, is below low boundary(High=<High value>, Low=<Low value>).  
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the flash usage percentage has fallen below the low boundary. Flash increases and decreases slightly with normal operation of the switch. Excessive permanent increases can lead to future problems.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1402

Message

```
<timestamp>, [FW-1402], <sequence-number>,, WARNING, <system-name>,  
<Label>, is above high boundary(High=<High value>, Low=<Low  
value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the flash usage percentage has risen above the high boundary. Flash increases and decreases slightly with normal operation of the switch. Excessive permanent increases can lead to future problems.

Recommended Action

You might have to remove some unwanted files to create some flash space. Run the **saveCore** command to remove files from the kernel space.

Severity

WARNING

FW-1403

Message

```
<timestamp>, [FW-1403], <sequence-number>,, INFO, <system-name>,  
<Label>, is between high and low boundaries(High=<High value>,  
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the flash usage percentage has changed from a value outside of the acceptable range to a value within the acceptable range. Flash increases and decreases slightly with normal operation of the switch. Excessive permanent increases can lead to future problems.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1424

Message

```
<timestamp>, [FW-1424], <sequence-number>,, WARNING, <system-name>,  
Switch status changed from <Previous state> to <Current state>.
```

Probable Cause

Indicates that the switch status is not in a healthy state. This occurred because of a policy violation. The valid state values are HEALTHY, MARGINAL, or DOWN.

Recommended Action

Run the **switchStatusShow** command to determine the policy violation.

Severity

WARNING

FW-1425

Message

```
<timestamp>, [FW-1425], <sequence-number>,, INFO, <system-name>,  
Switch status changed from <Bad state> to HEALTHY.
```

Probable Cause

Indicates that the switch status has changed to a healthy state. This occurred because a policy is no longer violated. The valid <bad state> values are MARGINAL or DOWN.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1426

Message

```
<timestamp>, [FW-1426], <sequence-number>,, WARNING, <system-name>,  
Switch status change contributing factor Power supply: <Number Bad>  
bad, <Number Missing> absent.
```

Probable Cause

Indicates that the switch status is not in a healthy state. This occurred because the number of faulty or missing power supplies is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended Action

Replace the faulty or missing power supply.

Severity

WARNING

FW-1427

Message

```
<timestamp>, [FW-1427], <sequence-number>,, WARNING, <system-name>,  
Switch status change contributing factor Power supply: <Number Bad>  
bad.
```

Probable Cause

Indicates that the switch status is not in a healthy state. This occurred because the number of faulty power supplies is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended Action

Replace the faulty power supply.

Severity

WARNING

FW-1428

Message

```
<timestamp>, [FW-1428], <sequence-number>,, WARNING, <system-name>,  
Switch status change contributing factor Power supply: <Number  
Missing> absent.
```

Probable Cause

Indicates that the switch status is not in a healthy state. This occurred because the number of missing power supplies is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended Action

Replace the missing power supply.

Severity

WARNING

FW-1429

Message

```
<timestamp>, [FW-1429], <sequence-number>,, WARNING, <system-name>,  
Switch status change contributing factor: Power supplies are not  
redundant.
```

Probable Cause

Indicates that the switch status is not in a healthy state. This occurred because the power supplies are not in the correct slots for redundancy.

Recommended Action

Rearrange the power supplies so that one is in an odd slot and other in an even slot to make them redundant.

Severity

WARNING

FW-1430

Message

```
<timestamp>, [FW-1430], <sequence-number>,, WARNING, <system-name>,  
Switch status change contributing factor Temperature sensor:  
<Number Bad> bad.
```

Probable Cause

Indicates that the switch status is not in a healthy state. This occurred because the number of faulty temperature sensors is greater than or equal to the policy set by the **switchStatusPolicySet** command. A temperature sensor is faulty when the sensor value is not in the acceptable range or is faulty.

Recommended Action

Replace the FRU with the faulty temperature sensor.

Severity

WARNING

FW-1431

Message

```
<timestamp>, [FW-1431], <sequence-number>,, WARNING, <system-name>,  
Switch status change contributing factor Fan: <Number Bad> bad.
```

Probable Cause

Indicates that the switch status is not in a healthy state. This occurred because the number of faulty fans is greater than or equal to the policy set by the **switchStatusPolicySet** command. A fan is faulty when sensor value is not in the acceptable range or is faulty.

Recommended Action

Replace the faulty or deteriorating fan FRUs.

Severity

WARNING

FW-1432

Message

```
<timestamp>, [FW-1432], <sequence-number>,, WARNING, <system-name>,  
Switch status change contributing factor WWN: <Number Bad> bad.
```

Probable Cause

Indicates that the switch status is not in a healthy state. This occurred because the number of faulty WWN cards is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended Action

Replace the faulty WWN card.

Severity

WARNING

FW-1433

Message

```
<timestamp>, [FW-1433], <sequence-number>,, WARNING, <system-name>,  
Switch status change contributing factor CP: CP non-redundant.
```

Probable Cause

Indicates that the switch status is not in a healthy state. This occurred because the number of faulty CPs is greater than or equal to the policy set by the **switchStatusPolicySet** command. The CPs are non-redundant.

If you power cycle a SAN Director 2/128 chassis in dual-domain configuration, and then reset the micro-switch of the active CP before the heartbeat is up, this will cause both CPs to come up in a non-redundant state.

Recommended Action

Run the **firmwareShow** command to verify that both CPs have compatible firmware levels. Run the **firmwareDownload** command to install the same level of firmware to both CPs. Replace any faulty CPs.

If you reset the micro-switch (the latch on the CP blade) on the active CP before the heartbeat was up on a power cycle, and the CPs came up non-redundant, then you should reboot the CPs again to clear the problem.

Severity

WARNING

FW-1434

Message

```
<timestamp>, [FW-1434], <sequence-number>,, WARNING, <system-name>,  
Switch status change contributing factor Blade: <Number Bad> blade  
failures.
```

Probable Cause

Indicates that the switch status is not in a healthy state. This occurred because the number of blade failures is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended Action

Replace the faulty blade.

Severity

WARNING

FW-1435

Message

```
<timestamp>, [FW-1435], <sequence-number>,, WARNING, <system-name>,  
Switch status change contributing factor Flash: usage out of range.
```

Probable Cause

Indicates that the switch status is not in a healthy state. This occurred because the flash usage is out of range. The policy was set using the **switchStatusPolicySet** command.

Recommended Action

Run the **saveCore** command to clear out the kernel flash. Refer to the *HP StorageWorks Fabric OS 5.x command reference guide* for more information about this command.

Severity

WARNING

FW-1436

Message

```
<timestamp>, [FW-1436], <sequence-number>,, WARNING, <system-name>,  
Switch status change contributing factor Marginal ports: <Num of  
marginal ports and the port numbers> marginal ports. (Port(s)  
<Unknown>)
```

Probable Cause

Indicates that the switch status is not in a healthy state. This occurred because the number of marginal ports is greater than or equal to the policy set using the **switchStatusPolicySet** command. A port is faulty when the port value for Link Loss, Synchronization Loss, Signal Loss, Invalid word, Protocol error, CRC error, Port state change or Buffer Limited Port is above the high boundary.

Recommended Action

Replace any faulty or deteriorating SFPs.

Severity

WARNING

FW-1437

Message

```
<timestamp>, [FW-1437], <sequence-number>,, WARNING, <system-name>,  
Switch status change contributing factor Faulty ports: <Num of  
faulty ports> faulty ports.
```

Probable Cause

Indicates that the switch status is not in a healthy state. This occurred because the number of faulty ports is greater than or equal to the policy set by the **switchStatusPolicySet** command. A port is considered faulty due to hardware failure such as a faulty SFP or port.

Recommended Action

Replace any faulty or deteriorating SFPs.

Severity

WARNING

FW-1438

Message

```
<timestamp>, [FW-1438], <sequence-number>,, WARNING, <system-name>,  
Switch status change contributing factor Missing SFPs: <Num of  
missing SFPs> missing SFPs.
```

Probable Cause

Indicates that the switch status is not in a healthy state. This occurred because the number of missing SFPs is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended Action

Run the **switchStatusPolicySet** command to modify the SFP policy or to add SFPs to the empty ports.

Severity

WARNING

FW-1439

Message

```
<timestamp>, [FW-1439], <sequence-number>,, WARNING, <system-name>,  
Switch status change contributing factor Switch offline.
```

Probable Cause

Indicates that the switch status is not in a healthy state. This occurred because the switch is offline.

Recommended Action

Run the **switchEnable** command.

Severity

WARNING

FW-1440

Message

```
<timestamp>, [FW-1440], <sequence-number>,, INFO, <system-name>,  
<FRU label> state has changed to <FRU state>.
```

Probable Cause

Indicates that the specified FRU's state has changed to "absent".

Recommended Action

No action is required. Verify that the event was planned.

Severity

INFO

FW-1441

Message

```
<timestamp>, [FW-1441], <sequence-number>,, INFO, <system-name>,  
<FRU label> state has changed to <FRU state>.
```

Probable Cause

Indicates that specified FRU's state has changed to "inserted". This means that a FRU is inserted but not powered on.

Recommended Action

No action is required. Verify that the event was planned.

Severity

INFO

FW-1442

Message

```
<timestamp>, [FW-1442], <sequence-number>,, INFO, <system-name>,  
<FRU label> state has changed to <FRU state>.
```

Probable Cause

Indicates that specified FRU's state has changed to "on".

Recommended Action

No action is required. Verify that the event was planned.

Severity

INFO

FW-1443

Message

```
<timestamp>, [FW-1443], <sequence-number>,, INFO, <system-name>,  
<FRU label> state has changed to <FRU state>.
```

Probable Cause

Indicates that specified FRU's state has changed to "off".

Recommended Action

No action is required. Verify that the event was planned.

Severity

INFO

FW-1444

Message

```
<timestamp>, [FW-1444], <sequence-number>,, WARNING, <system-name>,  
<FRU label> state has changed to <FRU state>.
```

Probable Cause

Indicates that the specified FRU's state has changed to "faulty".

Recommended Action

Replace the FRU.

Severity

WARNING

HAM error messages

HAM-1001

Message

```
<timestamp>, [HAM-1001], <sequence-number>,, CRITICAL,  
<system-name>, Standby CP is not Healthy, device <device name>  
status BAD, severity = <severity>
```

Probable Cause

Indicates that a standby CP device error is reported by the high-availability manager (HAM) Health Monitor, with a specific device and severity level. The severity level can be critical, major, or minor.

The active CP will continue to function normally, but because the standby CP is not healthy, nondisruptive failover is not possible.

Recommended Action

Reboot the standby CP blade by ejecting the card and reseating it.

If the problem persists, replace the standby CP.

Severity

CRITICAL

HAM-1002

Message

```
<timestamp>, [HAM-1002], <sequence-number>,, INFO, <system-name>,  
Standby CP is Healthy
```

Probable Cause

Indicates that all of the standby CP devices monitored by the HAM Health Monitor report no error.

Recommended Action

No action is required.

Severity

INFO

HAM-1004

Message

```
<timestamp>, [HAM-1004], <sequence-number>,, INFO, <system-name>,  
<Reboot Reason>
```

Probable Cause

This message records switch reboots that were not initiated by a user or by the **firmwareDownload** command. Some examples of errors that might initiate this message are hardware errors, software errors, compact flash errors, or memory errors. The possible values for <reboot reason> are:

- Processor rebooted - Hafailover
- Processor rebooted - Unknown

- Processor rebooted - Fastboot
- Processor rebooted - Giveup Master:SYSM
- Processor rebooted - CP Faulty:SYSM
- Processor rebooted - FirmwareDownload
- Processor rebooted - ConfigDownload:MS
- Processor rebooted - ChangeWWN:EM
- Processor rebooted - Reboot:WebTool
- Processor rebooted - Fastboot:WebTool
- Processor rebooted - Software Fault:Software Watchdog
- Processor rebooted - Software Fault:Kernel Panic
- Processor rebooted - Software Fault:ASSERT
- Processor rebooted - Reboot:SNMP
- Processor rebooted - Fastboot:SNMP
- Processor rebooted - Reboot
- Processor rebooted - Chassis Config
- Processor rebooted - Reboot:API
- Processor rebooted - Reboot:HAM
- Processor rebooted - EMFault:EM

Recommended Action

Check the error log on both CPs for additional messages that might indicate the reason for the reboot.

Severity

INFO

HAMK error messages

HAMK-1002

Message

```
<timestamp>, [HAMK-1002], <sequence-number>,, INFO, <system-name>,
Heartbeat down
```

Probable Cause

Indicates that the active CP blade determined that the standby CP blade is down. This might happen as a result of an operator-initiated action such as **firmwareDownload**, if the standby CP blade is reset or removed, or as a result of an error in the standby CP blade.

Recommended Action

Monitor the standby CP blade for a few minutes. If this message is due to a standby CP reboot, the message HAMK-1003 will display after the standby CP has completed the reboot successfully.

If the standby CP does not successfully connect to the active CP after 10 minutes, reboot the standby CP blade by ejecting the blade and reseating it.

Severity

INFO

HAMK-1003

Message

```
<timestamp>, [HAMK-1003], <sequence-number>,, INFO, <system-name>,  
Heartbeat up
```

Probable Cause

Indicates that the active CP blade detects the standby CP blade. This message indicates that the standby CP blade is available to take over in case a failure happens on the active CP blade. This message is typically seen when the standby CP blade reboots.

Recommended Action

No action is required. This message means that the standby CP is healthy.

Severity

INFO

HAMK-1004

Message

```
<timestamp>, [HAMK-1004], <sequence-number>,, INFO, <system-name>,  
Resetting standby CP (double reset may occur).
```

Probable Cause

Indicates that the standby CP is being reset due to a loss of heartbeat. This message is typically seen when the standby CP has been rebooted. Note that in certain circumstances a CP may experience a double reset and reboot twice in a row. A CP can recover automatically even if it has rebooted twice.

Recommended Action

No action is required.

Severity

INFO

HIL Error Messages

HIL-1101

Message

```
<timestamp>, [HIL-1101], <sequence-number>,, ERROR, <system-name>,  
Slot <slot number> faulted, <nominal voltage> (<measured voltage>  
is above threshold.
```

Probable Cause

Indicates that the blade voltage is above threshold. This message is specific to the Core Switch 2/64, SAN Director 2/128, or 4/256 SAN Director.

Recommended Action

Replace the faulty blade.

Severity

ERROR

HIL-1102

Message

```
<timestamp>, [HIL-1102], <sequence-number>,, ERROR, <system-name>,  
Slot <slot number> faulted, <nominal voltage> (<measured voltage>)  
is below threshold.
```

Probable Cause

Indicates that the blade voltage is below threshold. This message is specific to the Core Switch 2/64, SAN Director 2/128, or 4/256 SAN Director.

Recommended Action

Replace the faulty blade.

Severity

ERROR

HIL-1103

Message

```
<timestamp>, [HIL-1103], <sequence-number>,, ERROR, <system-name>,  
Blower <blower number> faulted, <nominal voltage> (<measured  
voltage>) is above threshold.
```

Probable Cause

Indicates that the fan voltage is above threshold.

Recommended Action

Run the **psShow** command to verify the power supply status.

Try to reseat the fan FRU and power supply FRU and verify that they are seated properly.

If the problem persists, replace the fan FRU or the power supply FRU as necessary.

Severity

ERROR

HIL-1104

Message

```
<timestamp>, [HIL-1104], <sequence-number>,, ERROR, <system-name>,  
Blower <blower number> faulted, <nominal voltage> (<measured  
voltage>) is below threshold.
```

Probable Cause

Indicates that the fan voltage is below threshold.

Recommended Action

Run the **psShow** command to verify the power supply status.

Try to reseal the fan FRU and power supply FRU and verify that they are seated properly.
If the problem persists, replace the fan FRU or the power supply FRU as necessary.

Severity

ERROR

HIL-1105

Message

```
<timestamp>, [HIL-1105], <sequence-number>,, ERROR, <system-name>,  
Switch error, <nominal voltage> (<measured voltage>) above  
threshold.
```

Probable Cause

Indicates that the switch voltage is above threshold. This message is specific to nonbladed switches and is not applicable to the Core Switch 2/64, SAN Director 2/128, or 4/256 SAN Director.

Recommended Action

For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V and SAN Switch 2/16V, the entire switch must be replaced, because these switches do not have FRUs.

For the SAN Switch 2/32 and SAN Switch 4/32, replace the motherboard FRU.

Severity

ERROR

HIL-1106

Message

```
<timestamp>, [HIL-1106], <sequence-number>,, ERROR, <system-name>,  
Switch error, <nominal voltage> (<measured voltage>) below  
threshold.
```

Probable Cause

Indicates that the switch voltage is below threshold. This message is specific to nonbladed switches and is not applicable to the Core Switch 2/64, SAN Director 2/128, or 4/256 SAN Director.

Recommended Action

For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V and SAN Switch 2/16V, the entire switch must be replaced, because these switches do not have FRUs.

For the SAN Switch 2/32 and SAN Switch 4/32, replace the motherboard FRU.

Severity

ERROR

HIL-1107

Message

```
<timestamp>, [HIL-1107], <sequence-number>,, CRITICAL,  
<system-name>, Switch faulted, <nominal voltage> (<measured  
voltage>) above threshold. System preparing for reset.
```

Probable Cause

Indicates that the switch voltage is above threshold. This message is specific to nonbladed switches and is not applicable to the Core Switch 2/64, SAN Director 2/128, or 4/256 SAN Director.

Recommended Action

For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V and SAN Switch 2/16V, the entire switch must be replaced, because these switches do not have FRUs.

For the SAN Switch 2/32 and SAN Switch 4/32, replace the motherboard FRU.

Severity

CRITICAL

HIL-1108

Message

```
<timestamp>, [HIL-1108], <sequence-number>,, CRITICAL,  
<system-name>, Switch faulted, <nominal voltage> (<measured  
voltage>) below threshold. System preparing for reset.
```

Probable Cause

Indicates that the switch voltage is below threshold. This message is specific to nonbladed switches and is not applicable to the Core Switch 2/64, SAN Director 2/128, or 4/256 SAN Director.

Recommended Action

For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V and SAN Switch 2/16V, the entire switch must be replaced, because these switches do not have FRUs.

For the SAN Switch 2/32 and SAN Switch 4/32, replace the motherboard FRU.

Severity

CRITICAL

HIL-1201

Message

```
<timestamp>, [HIL-1201], <sequence-number>,, WARNING,  
<system-name>, Blower <blower number>, speed (<measured speed> RPM)  
above threshold.
```

Probable Cause

Indicates that the fan speed (in RPM) has risen above the maximum threshold. A high speed does not necessarily mean that the fan is faulty.

Recommended Action

Run the **tempShow** command to verify that the switch temperatures are within operational range. Refer to the hardware reference manual for the temperature range of your switch.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Run the **fanShow** command to monitor the speed of the fan generating this error.

For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, if the fan problem causes the switch to have temperature problems, you must replace the entire switch.

For the SAN Switch 2/32 and SAN Switch 4/32, if the fan problem causes the switch to have temperature problems, replace the fan FRU.

Severity

WARNING

HIL-1202

Message

```
<timestamp>, [HIL-1202], <sequence-number>,, ERROR, <system-name>,  
Blower <blower number> faulted, speed (<measured speed> RPM) below  
threshold.
```

Probable Cause

Indicates that the specified fan speed (in RPM) has fallen below the minimum threshold.

Recommended Action

Run the **tempShow** command to verify that the switch temperatures are within operational range. Refer to the hardware reference manual for the temperature range of your switch.

Run the **fanShow** command to monitor the speed of the fan generating this error.

For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, if the fan problem causes the switch to have temperature problems, you must replace the entire switch.

For the SAN Switch 2/32 and SAN Switch 4/32, if the fan problem causes the switch to have temperature problems, replace the fan FRU.

Severity

ERROR

HIL-1203

Message

```
<timestamp>, [HIL-1203], <sequence-number>,, ERROR, <system-name>,  
Fan <fan number> faulted, speed (<measured speed> RPM) above  
threshold.
```

Probable Cause

Indicates that the specified fan speed (in RPM) has risen above the maximum threshold. A high speed does not necessarily mean that the fan is faulty.

Recommended Action

Run the **tempShow** command to verify that the switch temperatures are within operational range. Refer to the hardware reference manual for the temperature range of your switch.

Run the **fanShow** command to monitor the speed of the fan generating this error.

For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, if the fan problem causes the switch to have temperature problems, you must replace the entire switch.

For the SAN Switch 2/32 and SAN Switch 4/32, if the fan problem causes the switch to have temperature problems, replace the fan FRU.

Severity

ERROR

HIL-1204

Message

```
<timestamp>, [HIL-1204], <sequence-number>,, ERROR, <system-name>,  
Fan <fan number> faulted, speed (<measured speed> RPM) below  
threshold.
```

Probable Cause

Indicates that the specified fan speed (in RPM) has fallen below the minimum threshold. This message is specific to nonbladed switches and is not applicable to the Core Switch 2/64, SAN Director 2/128, or 4/256 SAN Director.

Recommended Action

Run the **tempShow** command to verify that the switch temperatures are within operational range. Refer to the hardware reference manual for the temperature range of your switch.

Run the **fanShow** command to monitor the speed of the fan generating this error.

For the SAN Switch 2/32 and SAN Switch 4/32, if the fan problem is causing temperature problems on the switch, replace the fan FRU.

For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V and SAN Switch 2/16V, if the fan problem is causing temperature problems on the switch, the entire switch must be replaced, because these switches do not have FRUs.

Severity

ERROR

HIL-1205

Message

```
<timestamp>, [HIL-1205], <sequence-number>,, ERROR, <system-name>,  
Fan <fan number> sensor <sensor number>, speed (<measured speed>  
RPM) above threshold.
```

Probable Cause

Indicates that the specified fan speed (in RPM) has risen above the maximum threshold. A high speed does not necessarily mean that the fan is faulty.

Recommended Action

Run the **tempShow** command to verify that the switch temperatures are within operational range. Refer to the hardware reference manual for the temperature range of your switch.

Run the **fanShow** command to monitor the speed of the fan generating this error.

For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, if the fan problem is causing temperature problems on the switch, you must replace the entire switch.

For the SAN Switch 2/32 and SAN Switch 4/32, if the fan problem is causing temperature problems on the switch, replace the fan FRU.

Severity

ERROR

HIL-1206

Message

```
<timestamp>, [HIL-1206], <sequence-number>,, ERROR, <system-name>,  
Fan <fan number> sensor <sensor number> speed (<measured speed>  
RPM) below threshold.
```

Probable Cause

Indicates that the specified fan speed (in RPM) has fallen below the minimum threshold. This problem can quickly cause the switch to overheat. This message is specific to nonbladed switches and is not applicable to the Core Switch 2/64, SAN Director 2/128, or 4/256 SAN Director.

Recommended Action

Run the **tempShow** command to verify that the switch temperatures are within operational range. Refer to the hardware reference manual for the temperature range of your switch.

Run the **fanShow** command to monitor the speed of the fan generating this error.

For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, if the fan problem is causing temperature problems on the switch, you must replace the entire switch.

For the SAN Switch 2/32 and SAN Switch 4/32, if the fan problem is causing temperature problems on the switch, replace the fan FRU.

Severity

ERROR

HIL-1207

Message

```
<timestamp>, [HIL-1207], <sequence-number>,, ERROR, <system-name>,  
Fan <fan number> is faulty.
```

Probable Cause

Indicates that the fan is faulty.

Recommended Action

Run the **tempShow** command to check if the switch temperatures are too high. Refer to the hardware reference manual for the temperature range of your switch.

Run the **fanShow** command to verify that the fan is faulty.

For the SAN Switch 2/32 and SAN Switch 4/32, replace the fan FRU.

For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V and SAN Switch 2/16V, the entire switch must be replaced, because these switches do not have FRUs.

Severity

ERROR

HIL-1301

Message

```
<timestamp>, [HIL-1301], <sequence-number>,, ERROR, <system-name>,  
1 blower failed. Replace failed blower assembly immediately.
```

Probable Cause

Indicates that a fan FRU has failed. This message is often preceded by a low speed error message. This problem can quickly cause the switch to overheat.

Recommended Action

Run the **tempShow** command to check if the switch temperatures are too high. Refer to the hardware reference manual for the temperature range of your switch.

Run the **fanShow** command to verify that the fan is faulty.

For the SAN Switch 2/32 and SAN Switch 4/32, replace the fan FRU.

For the 4/8 SAN Switch, 4/16 SAN Switch, Brocade 4Gb SAN Switch for HP p-Class Blade, SAN Switch 2/8V and SAN Switch 2/16V, the entire switch must be replaced, because these switches do not have FRUs.

Severity

ERROR

HIL-1302

Message

```
<timestamp>, [HIL-1302], <sequence-number>,, ERROR, <system-name>,  
<count> blowers failed. Replace failed blower assemblies  
immediately.
```

Probable Cause

Indicates that multiple fan FRUs have failed on a switch. This message is often preceded by a low fan speed message.

Recommended Action

Run the **tempShow** command to check if the switch temperatures are too high. Refer to the hardware reference manual for the temperature range of your switch.

Run the **fanShow** command to verify that the fans are faulty.

For the SAN Switch 2/32 and SAN Switch 4/32, replace the fan FRU.

For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V and SAN Switch 2/16V, the entire switch must be replaced, because these switches do not have FRUs.

Severity

ERROR

HIL-1303

Message

```
<timestamp>, [HIL-1303], <sequence-number>,, ERROR, <system-name>,  
One fan failed. Replace failed fan FRU immediately.
```

Probable Cause

Indicates that a fan FRU has failed. This message is often preceded by a low fan speed message.

Recommended Action

Run the **tempShow** command to check if the switch temperatures are too high. Refer to the hardware reference manual for the temperature range of your switch.

Run the **fanShow** command to verify that the fan is faulty.

For the SAN Switch 2/32 and SAN Switch 4/32, replace the fan FRU.

For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V and SAN Switch 2/16V, the entire switch must be replaced, because these switches do not have FRUs.

Severity

ERROR

HIL-1304

Message

```
<timestamp>, [HIL-1304], <sequence-number>,, ERROR, <system-name>,  
Two fans failed. Replace failed fan FRUs immediately.
```

Probable Cause

Indicates that multiple fan FRUs have failed. This message is often preceded by a low fan speed message.

Recommended Action

Run the **tempShow** command to check if the switch temperatures are too high. Refer to the hardware reference manual for the temperature range of your switch.

Run the **fanShow** command to verify that the fan is faulty.

For the SAN Switch 2/32 and SAN Switch 4/32, replace the fan FRU.

For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V and SAN Switch 2/16V, the entire switch must be replaced, because these switches do not have FRUs.

Severity

ERROR

HIL-1305

Message

```
<timestamp>, [HIL-1305], <sequence-number>,, ERROR, <system-name>,  
One or two fan(s) failed. Replace failed fan FRU(s) immediately.
```

Probable Cause

Indicates that multiple fan FRUs have failed. This message is often preceded by a low fan speed message.

Recommended Action

Run the **tempShow** command to check if the switch temperatures are too high. Refer to the hardware reference manual for the temperature range of your switch.

Run the **fanShow** command to verify that the fans are faulty.

For the SAN Switch 2/32 and SAN Switch 4/32, replace the fan FRU.

For the 4/8 SAN Switch, SAN Switch 2/8V and SAN Switch 2/16V, the entire switch must be replaced, because these switches do not have FRUs.

Severity

ERROR

HIL-1306

Message

```
<timestamp>, [HIL-1306], <sequence-number>,, ERROR, <system-name>,  
Three fans failed. Replace failed fan FRUs immediately.
```

Probable Cause

Indicates that three fan FRUs have failed. This message is often preceded by a low fan speed message.

Recommended Action

Run the **tempShow** command to check if the switch temperatures are too high. Refer to the hardware reference manual for the temperature range of your switch.

Run the **fanShow** command to verify that the fans are faulty.

For the SAN Switch 2/32 and SAN Switch 4/32, replace the fan FRU.

For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V and SAN Switch 2/16V, the entire switch must be replaced, because these switches do not have FRUs.

Severity

ERROR

HIL-1307

Message

```
<timestamp>, [HIL-1307], <sequence-number>,, ERROR, <system-name>,  
Four or five fans failed. Replace failed fan FRUs immediately.
```

Probable Cause

Indicates that multiple fan FRUs have failed. This message is often preceded by a low fan speed message.

Recommended Action

Run the **tempShow** command to check if the switch temperatures are too high. Refer to the hardware reference manual for the temperature range of your switch.

Run the **fanShow** command to verify that the fans are faulty.

For the SAN Switch 2/32 and SAN Switch 4/32, replace the fan FRU.

For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V and SAN Switch 2/16V, the entire switch must be replaced, because these switches do not have FRUs.

Severity

ERROR

HIL-1308

Message

```
<timestamp>, [HIL-1308], <sequence-number>,, ERROR, <system-name>,  
All fans failed. Replace failed fan FRUs immediately.
```

Probable Cause

Indicates that all fans have failed. This message is often preceded by a low fan speed message.

Recommended Action

Run the **tempShow** command to check if the switch temperatures are too high. Refer to the hardware reference manual for the temperature range of your switch.

Run the **fanShow** command to verify that the fans are faulty.

For the SAN Switch 2/32 and SAN Switch 4/32, replace the fan FRU.

For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V and SAN Switch 2/16V, the entire switch must be replaced, because these switches do not have FRUs.

Severity

ERROR

HIL-1309

Message

```
<timestamp>, [HIL-1309], <sequence-number>,, ERROR, <system-name>,  
<count> fan FRU(s) failed. Replace failed fan FRU(s) immediately.
```

Probable Cause

Indicates that multiple fans have failed. This message is often preceded by a low fan speed message.

Recommended Action

Run the **tempShow** command to check if the switch temperatures are too high. Refer to the hardware reference manual for the temperature range of your switch.

Run the **fanShow** command to verify that the fans are faulty.

For the SAN Switch 2/32 and SAN Switch 4/32, replace the fan FRU.

For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V and SAN Switch 2/16V, the entire switch must be replaced, because these switches do not have FRUs.

Severity

ERROR

HIL-1310

Message

```
<timestamp>, [HIL-1310], <sequence-number>,, WARNING,  
<system-name>, <count> fan(s) faulty.
```

Probable Cause

Indicates that multiple fans have failed. This message is often preceded by a low fan speed message.

Recommended Action

For the SAN Switch 2/32 and SAN Switch 4/32, replace the fan FRU.

For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V and SAN Switch 2/16V, the entire switch must be replaced, because these switches do not have FRUs.

Severity

WARNING

HIL-1401

Message

```
<timestamp>, [HIL-1401], <sequence-number>,, WARNING,  
<system-name>, One fan FRU missing. Install fan FRU immediately.
```

Probable Cause

Indicates that one fan FRU has been removed.

Recommended Action

Install the missing fan FRU.

Severity

WARNING

HIL-1402

Message

```
<timestamp>, [HIL-1402], <sequence-number>,, WARNING,  
<system-name>, Two fan FRUs missing. Install fan FRUs immediately.
```

Probable Cause

Indicates that two fan FRUs have been removed.

Recommended Action

Install the missing fan FRUs immediately.

Severity

WARNING

HIL-1403

Message

```
<timestamp>, [HIL-1403], <sequence-number>,, WARNING,  
<system-name>, All fan FRUs missing. Install fan FRUs immediately.
```

Probable Cause

Indicates that all fan FRUs have been removed.

Recommended Action

Install the missing fan FRUs immediately.

Severity

WARNING

HIL-1404

Message

```
<timestamp>, [HIL-1404], <sequence-number>,, WARNING,  
<system-name>, <count> fan FRU(s) missing. Install fan FRU(s)  
immediately.
```

Probable Cause

Indicates that one or more fan FRUs have been removed.

Recommended Action

Install the missing fan FRUs immediately.

Severity

WARNING

HIL-1501

Message

```
<timestamp>, [HIL-1501], <sequence-number>,, WARNING,  
<system-name>, Slot <slot number>, high temperature (<measured  
temperature>).
```

Probable Cause

Indicates that the temperature of this blade has risen above the warning threshold. This message only occurs on the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.

Recommended Action

Run the **tempShow** command to monitor switch temperatures. Refer to the hardware reference manual for the temperature range of your switch.

Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Severity

WARNING

HIL-1502

Message

```
<timestamp>, [HIL-1502], <sequence-number>,, CRITICAL,  
<system-name>, Slot <slot number>, high temperature (<measured  
temperature>). Unit will be shut down in 2 minutes if temperature  
remains high.
```

Probable Cause

Indicates that the temperature of this blade has risen above the critical threshold. This usually follows a high-temperature message. This message only occurs on the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.

Recommended Action

Run the **tempShow** command to monitor switch temperatures. Refer to the hardware reference manual for the temperature range of your switch.

Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

If the message persists, replace the blade.

Severity

CRITICAL

HIL-1503

Message

```
<timestamp>, [HIL-1503], <sequence-number>,, CRITICAL,  
<system-name>, Slot <slot number>, unit shutting down.
```

Probable Cause

Indicates that the temperature of this blade has risen above the maximum threshold for at least two minutes. The blade is shut down to prevent further damage. This usually follows a high-temperature warning message. This message only occurs on the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.

Recommended Action

Run the **tempShow** command to monitor switch temperatures. Refer to the hardware reference manual for the temperature range of your switch.

Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

If the message persists, replace the faulty blade.

Severity

CRITICAL

HIL-1504

Message

```
<timestamp>, [HIL-1504], <sequence-number>,, INFO, <system-name>,  
System within normal temperature specifications (<measured  
temperature> C).
```

Probable Cause

Indicates that temperatures in the system have returned to normal.

Recommended Action

No action is required.

Severity

INFO

HIL-1505

Message

```
<timestamp>, [HIL-1505], <sequence-number>,, WARNING,  
<system-name>, High temperature (<measured temperature> C) exceeds  
environmental specifications.
```

Probable Cause

Indicates that temperatures in the system have risen above the warning threshold.

Recommended Action

Run the **tempShow** command to monitor switch temperatures. Refer to the hardware reference manual for the temperature range of your switch.

Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Severity

WARNING

HIL-1506

Message

```
<timestamp>, [HIL-1506], <sequence-number>,, CRITICAL,  
<system-name>, High temperature (<measured temperature> C) exceeds  
system temperature limit. System will shut down within 2 minutes.
```

Probable Cause

Indicates that temperatures in the system have risen above the critical threshold.

Recommended Action

Run the **tempShow** command to monitor switch temperatures. Refer to the hardware reference manual for the temperature range of your switch.

Run the **fanShow** command to verify all the fans are working properly.

Replace any deteriorating fan FRUs.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Severity

CRITICAL

HIL-1507

Message

```
<timestamp>, [HIL-1507], <sequence-number>,, CRITICAL,  
<system-name>, High temperature warning time expired. System  
preparing for shutdown.
```

Probable Cause

Indicates that temperatures in the system have risen above the critical threshold. This message only occurs on the SAN Switch 2/16V, SAN Switch 2/8V, and SAN Switch 2/32.

Recommended Action

Temperatures have probably caused damage to the switch and the system shuts down automatically. To help prevent future problems, make sure that all the fans are working properly.

Run the **tempShow** command to verify proper switch temperatures. Refer to the hardware reference manual for the temperature range of your switch.

Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Severity

CRITICAL

HIL-1508

Message

```
<timestamp>, [HIL-1508], <sequence-number>,, CRITICAL,  
<system-name>, Fan faulty warning time expired. System preparing  
for shutdown.
```

Probable Cause

Indicates that temperatures in the system have remained above the critical threshold too long.

Recommended Action

Temperatures have probably caused damage to the switch and the system shuts down automatically. To help prevent future problems, make sure that all the fans are working properly.

Run the **tempShow** command to monitor switch temperatures. Refer to the hardware reference manual for the temperature range of your switch.

Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Severity

CRITICAL

HIL-1509

Message

```
<timestamp>, [HIL-1509], <sequence-number>,, CRITICAL,  
<system-name>, High temperature (<measured temperature> C). Warning  
time expired. System preparing for shutdown.
```

Probable Cause

Indicates that temperatures in the system have risen above the critical threshold.

Recommended Action

Temperatures have probably caused damage to the switch and the system shuts down automatically. To help prevent future problems, make sure that all the fans are working properly.

Run the **tempShow** command to monitor switch temperatures. Refer to the hardware reference manual for the temperature range of your switch.

Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Severity

CRITICAL

HIL-1601

Message

```
<timestamp>, [HIL-1601], <sequence-number>,, ERROR, <system-name>,  
Using backup temperature sensor. Service immediately.
```

Probable Cause

Indicates that temperature readings from the primary sensor are out of range.

Recommended Action

Run the **fanShow** command to verify that all fans are operating correctly. Replace any deteriorating fan FRUs.

Run the **tempShow** command to verify temperature values. If any sensor is too high, monitor the switch. Try rebooting or power cycling the switch.

Severity

ERROR

HIL-1602

Message

```
<timestamp>, [HIL-1602], <sequence-number>,, CRITICAL,  
<system-name>, All temperature sensors failed. Service immediately.
```

Probable Cause

Indicates that temperature readings from all sensors are out of range.

Recommended Action

Run the **fanShow** command to verify that all fans are operating correctly. Replace any deteriorating fan FRUs.

Run the **tempShow** command to verify temperature values. If any sensor is too high, monitor the switch. Try rebooting or power cycling the switch.

Severity

CRITICAL

HLO error messages

HLO-1001

Message

```
<timestamp>, [HLO-1001], <sequence-number>,, ERROR, <system-name>,  
Incompatible Inactivity timeout <dead timeout> from port <port  
number>, correct value <value>
```

Probable Cause

Indicates that the HLO message was incompatible with the value specified in the FSPF protocol. The HP StorageWorks switch will not accept FSPF frames from the remote switch.

In the Fabric OS, the HLO dead timeout value is not configurable, so this error can only occur when the HP StorageWorks switch is connected to a switch from another manufacturer.

Recommended Action

The dead timeout value of the remote switch must be compatible with the value specified in the FSPF protocol. Refer to the documentation of the other manufacturer's switch to change this value.

Severity

ERROR

HLO-1002

Message

```
<timestamp>, [HLO-1002], <sequence-number>,, ERROR, <system-name>,  
Incompatible Hello timeout <HLO timeout> from port <port number>,  
correct value <correct value>
```

Probable Cause

Indicates that the HLO message was incompatible with the value specified in the FSPF protocol. The HP StorageWorks switch will not accept FSPF frames from the remote switch.

In the Fabric OS, the HLO timeout value is not configurable, so this error can only occur when the HP StorageWorks switch is connected to a switch from another manufacturer.

Recommended Action

The HLO timeout value of the remote switch must be compatible with the value specified in the FSPF protocol. Refer to the documentation of the other manufacturer's switch to change this value.

Severity

ERROR

HLO-1003

Message

```
<timestamp>, [HLO-1003], <sequence-number>,, ERROR, <system-name>,  
Invalid Hello received from port <port number>, Domain = <domain  
ID>, Remote Port = <remote port ID>
```

Probable Cause

Indicates that the HLO message received was invalid and the frame was dropped. The HP StorageWorks switch will not accept FSPF frames from the remote switch.

The switch has received an invalid HLO because either the domain or port number in the HLO message has an invalid value. This error can only occur when the HP StorageWorks switch is connected to a switch from another manufacturer.

Recommended Action

The HLO message of the remote switch must be compatible with the value specified in the FSPF protocol. Refer to the documentation of the other manufacturer's switch to change this value.

Severity

ERROR

HMON error messages

HMON-1001

Message

```
<timestamp>, [HMON-1001], <sequence-number>,, CRITICAL,  
<system-name>, <Failure description>
```

Probable Cause

Indicates that there was a problem reading the configuration file from the nonvolatile storage device. This could be the result of a missing file or a corrupt file system.

The *failure description* is "configuration file error".

Recommended Action

Run the **firmwareDownload** command to reinstall the firmware to your switch.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

CRITICAL

HTTP error messages

HTTP-1001

Message

```
<timestamp>, [HTTP-1001], <sequence-number>,, INFO, <system-name>,  
Switch PIDformat has changed to <current PID format>.
```

Probable Cause

Indicates that the PID format was changed by the administrator.

Recommended Action

No action is required. For more information on PID, format refer to the *HP StorageWorks Fabric OS 5.x administrator's guide*.

Severity

INFO

KSWD error messages

KSWD-1003

Message

```
<timestamp>, [KSWD-1003], <sequence-number>,, WARNING,  
<system-name>, kSWD: <Warning message>
```

Probable Cause

Indicates a warning state within the system.

A critical application error was reported in the watchdog subsystem. This message is used to convey information that might be of interest to the customer regarding the state of the system. Refer to the string at the end of the error message for specific information. The switch will reboot (on single-CP switches) or failover (on dual-CP switches).

The error message might be any one of the following:

U R HERE

- <Detected unexpected termination of: <daemon name>>
Probable Cause: One of the critical daemons ended unexpectedly.
- <<daemon name> failed to refresh SWD*** Sending SIGABRT to pid <process id number>>
Probable Cause: One of the critical daemons is found to be nonresponsive; sending signal abort.

Recommended Action

Run the savecore command to find if any core files were created. If a core file is found, FTP all core files to a secure server location.

Copy the error message, any core file information, and contact your switch service provider.

Severity

WARNING

KTRC error messages

KTRC-1001

Message

```
<timestamp>, [KTRC-1001], <sequence-number>,, WARNING,  
<system-name>, Dump memory size exceeds dump file size
```

Probable Cause

Indicates that the dump memory size has exceeded the dump file size.

Recommended Action

No action is required.

Severity

WARNING

KTRC-1002

Message

```
<timestamp>, [KTRC-1002], <sequence-number>,, INFO, <system-name>,  
Concurrent trace dumping.
```

Probable Cause

Indicates that the initial background dump has not completed.

Recommended Action

No action is required.

Severity

INFO

KTRC-1003

Message

```
<timestamp>, [KTRC-1003], <sequence-number>,, ERROR, <system-name>,  
Cannot open ATA dump device
```

Probable Cause

Indicates that the ATA dump driver is not initialized properly.

Recommended Action

No action is required.

Severity

ERROR

KTRC-1004

Message

```
<timestamp>, [KTRC-1004], <sequence-number>,, ERROR, <system-name>,  
Cannot write to ATA dump device
```

Probable Cause

Indicates that the write boundry in the ATA dump device has been exceeded.

Recommended Action

No action is required.

Severity

ERROR

LOG Error Messages

LOG-1000

Message

```
<timestamp>, [LOG-1000], <sequence-number>,, INFO, <system-name>,  
Previous message repeated <repeat count> time(s)
```

Probable Cause

Indicates that the previous message repeated the number of times specified by the repeat count.

Recommended Action

No action is required.

Severity

INFO

LOG-1001

Message

```
<timestamp>, [LOG-1001], <sequence-number>,, CRITICAL,  
<system-name>, A log message was dropped
```

Probable Cause

Indicates that a log message was dropped.

Recommended Action

Run the **reboot** command for nonbladed switches or the **haFailover** command on bladed switches.

Run the **saveCore** command to FTP core files to a server location. It is normal behavior if there are no core files to transfer.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

CRITICAL

LOG-1002

Message

```
<timestamp>, [LOG-1002], <sequence-number>,, CRITICAL,  
<system-name>, A log message was dropped
```

Probable Cause

Indicates that a message was not recorded by the error logging system. A trace dump file is created. The message might still be visible through SNMP or other management tools.

Recommended Action

Run the **reboot** command for nonbladed switches or the **haFailover** command on bladed switches.

Run the **saveCore** command to FTP core files to a server location. It is normal behavior if there are no core files to transfer.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

CRITICAL

LSDB Error Messages

LSDB-1001

Message

```
<timestamp>, [LSDB-1001], <sequence-number>,, ERROR, <system-name>,  
Link State ID <link state ID> out of range
```

Probable Cause

Indicates that the link state database ID is out of the acceptable range. The valid *link state ID* is the same as the valid domain ID, whose range is from 1 through 239. The switch will discard the record because it is not supported.

Recommended Action

No action is required.

Severity

ERROR

LSDB-1002

Message

```
<timestamp>, [LSDB-1002], <sequence-number>,, INFO, <system-name>,  
Local Link State Record reached max incarnation#
```

Probable Cause

Indicates that the local link state database reached the maximum incarnations.

An "incarnation" is a progressive number that identifies the most recent version of the LSR (link state record). The switch generates its local link state record when first enabled.

Recommended Action

No action is required. The incarnation count will begin again at 0x80000001 after reaching 0x7FFFFFFF.

Severity

INFO

LSDB-1003

Message

```
<timestamp>, [LSDB-1003], <sequence-number>,, CRITICAL,  
<system-name>, No database entry for local Link State Record,  
domain <local domain>
```

Probable Cause

Indicates that there is no local link state record entry in the link state database. The switch should always generate its own local entry when starting up.

An "incarnation" is a progressive number that identifies the most recent version of the LSR (link state record). The switch generates its local link state record when first enabled. By disabling and enabling the switch, a new local link state record is generated.

Recommended Action

Run the **switchDisable** and **switchEnable** commands. A new local link state record is generated during the switch enable.

Severity

CRITICAL

LSDB-1004

Message

```
<timestamp>, [LSDB-1004], <sequence-number>,, WARNING,  
<system-name>, No Link State Record for domain <local domain>
```

Probable Cause

Indicates that there is no link state record for the specified *local domain*.

Recommended Action

No action is required. The other switch will pass the LSD when the fabric has become stable.

Severity

WARNING

MFIC Error Messages

MFIC-1001

Message

```
<timestamp>, [MFIC-1001], <sequence-number>,, ERROR, <system-name>,  
failure at sysmod_scn registry rc= <failure reason>
```

Probable Cause

Indicates that the system is temporarily out of resources.

Recommended Action

This message is often transitory, and requires no action.

If the message persists, run a switch **reboot** or an **haFailover** (if applicable).

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

MFIC-1002

Message

```
<timestamp>, [MFIC-1002], <sequence-number>,, INFO, <system-name>,  
Chassis FRU header not programmed for switch NID, using defaults  
(applies only to FICON environments).
```

Probable Cause

Indicates that custom switch node descriptor (NID) fields have not been programmed in nonvolatile storage. The default values are used. The Switch NID is used only in the following SB ELS frames: Request Node Identification Data (RNID) and Registered Link Incident Record (RLIR). The use of SB-3 link incident registration and reporting is typically limited to FICON environments.

Recommended Action

No action is required if SB-3 link incident registration and reporting is not used by the host or if default values are desired for the switch node descriptor fields.

Severity

INFO

MFIC-1003

Message

```
<timestamp>, [MFIC-1003], <sequence-number>,, WARNING,  
<system-name>, Effective Insistent domain ID for the fabric changed  
from <state> to <state>
```

Probable Cause

Indicates that one or more switches joined the fabric with a different insistent domain ID (IDID) mode setting than the current effective IDID mode for the fabric. This message also occurs when the IDID for the fabric has been turned on or off. The possible values for state are:

- On
- Off

Recommended Action

IDID mode is a fabric-wide mode; make sure that any switches added to the fabric are configured with the same IDID mode as the fabric. If you are enabling or disabling IDID mode, this message is for information purposes only, and no action is required. IDID mode can be set using the **configure** command in the CLI or checking the Advanced Web Tools **Switch Admin > Configure Tab > Fabric Subtab > Insistent Domain ID Mode** checkbox. The switch must be disabled to change the IDID mode.

Severity

WARNING

MPTH Error Messages

MPTH-1001

Message

```
<timestamp>, [MPTH-1001], <sequence-number>,, ERROR, <system-name>,  
Null parent, lsId = <number>
```

Probable Cause

Indicates that a null parent was reported. MPATH uses a tree structure in which the parent is used to connect to the root of the tree.

Recommended Action

No action is required.

Severity

ERROR

MPTH-1002

Message

```
<timestamp>, [MPTH-1002], <sequence-number>,, ERROR, <system-name>,  
Null lsrP, lsId = <ls ID number>
```

Probable Cause

Indicates that a link state record is null.

Recommended Action

No action is required.

Severity

ERROR

MPTH-1003

Message

```
<timestamp>, [MPTH-1003], <sequence-number>,, WARNING,  
<system-name>, No minimum cost path in candidate list
```

Probable Cause

Indicates that the FSPF module has determined that there is no minimum cost path (MPath) available in the candidate list.

Recommended Action

No action is required.

Severity

WARNING

MQ Error Messages

MQ-1004

Message

```
<timestamp>, [MQ-1004], <sequence-number>,, ERROR, <system-name>,  
mqRead, queue = <queue name>, queue ID = <queue ID>, type = <message  
type>
```


Probable Cause

Indicates that an unexpected message has been received in the specified message queue. The *queue name* is always fspf_q. The *queue ID* and *message type* can be any of the following:

- 2 - MSG_TX
- 3 - MSG_INTR
- 4 - MSG_STR
- 6 - MSG_ASYNC_IU
- 7 - MSG_LINIT_IU
- 8 - MSG_RSCN
- 9 - MSG_IOCTL
- 10 - MSG_ACCEPT
- 11 - MSG_IU_FREE
- 12 - MSG_US
- 13 - MSG_EXT_RSCN
- 14 - MSG_RDTS_START
- 15 - MSG_RDTS_SENDEFP
- 16 - MSG_RDTS_RESET

Recommended Action

No action is required.

Severity

ERROR

MS Error Messages

MS-1001

Message

```
<timestamp>, [MS-1001], <sequence-number>,, WARNING, <system-name>,  
MS Platform Segmented port=<port number>(<reason for segmentation>  
<domain>)
```

Probable Cause

Indicates that the management server (MS) has segmented from another switch *domain* at the specified *port number* due to errors or inconsistencies defined in the MS platform service.

Recommended Action

Reboot or power cycle the switch.

Severity

WARNING

MS-1002

Message

```
<timestamp>, [MS-1002], <sequence-number>,, INFO, <system-name>, MS  
Platform Service Unstable(<message string><domain number>)
```

Probable Cause

The MS platform service is unstable.

The *<message string>* can be one of the following:

- *<No Resp for GCAP from>*
The switch did not respond to a request for GCAP (MS Get Capabilities) command.
Recommended Action: No action is required.
- *<GCAP sup but not PL by>*
The GCAP (MS Get Capabilities) is supported but the flag for MS platform service is not set.
Recommended Action: Set the flag for the MS Platform Service.
- *<GCAP Rejected (reason =BUSY) by>*
The GCAP (MS Get Capabilities) is not supported by another switch.
Recommended Action: Upgrade the firmware level on the switch to a level that supports RCS.
- *<Reject EXGPLDB from>*
The request to the exchange platform database was rejected. The remote switch might be busy.
Recommended Action: Wait a few minutes and try the command again.

The *<domain number>* is the target domain that caused error.

Recommended Action

The recommended actions are as follows:

- *<No Resp for GCAP from>*
No action is required.
- *<GCAP sup but not PL by>*
Set the flag for the MS Platform Service.
- *<GCAP Rejected (reason =BUSY) by>*
Run the **firmwareDownload** command to upgrade the firmware level on the switch to a level that supports RCS. RCS is supported in Fabric OS v2.6, v3.1 and greater, and v4.1 and greater.
- *<Reject EXGPLDB from>*
Wait a few minutes and try the command again.

Severity

INFO

MS-1003

Message

```
<timestamp>, [MS-1003], <sequence-number>,, INFO, <system-name>, MS  
detected Unstable Fabric(<message string><domain number>).
```

Probable Cause

Indicates that MS detected an unstable fabric; the command or operation might not be successfully completed. This message is often transitory. The fabric might be reconfiguring, forming, or merging.

The *message string* can be one of the following:

- *<DOMAIN_INVALID for a req from>*
The domain is invalid for a request.
- *<No WWN for>*
Unable to acquire the World Wide Name (WWN) for the corresponding domain.

The *domain number* is the target domain that caused error.

Recommended Action

Wait a few minutes and try the operation again.

Run the **fabricShow** command or the **secFabricShow** command to verify that the number of domains matches the Management Server known domains.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

INFO

MS-1004

Message

```
<timestamp>, [MS-1004], <sequence-number>,, INFO, <system-name>, MS  
detected ONLY 1 Domain(d=<domain in local resource>).
```

Probable Cause

Indicates that MS detected an unstable count of domains in its own local resource. This message is often transitory. The fabric might be reconfiguring, forming, or merging.

Recommended Action

Wait a few minutes and try the operation again.

Run the **fabricShow** command or the **secFabricShow** command to verify that the number of domains matches the Management Server known domains.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

INFO

MS-1005

Message

```
<timestamp>, [MS-1005], <sequence-number>,, ERROR, <system-name>,  
MS Invalid CT Response from d=<domain>
```

Probable Cause

Indicates that MS received an invalid common transport (CT) response from switch *domain*. MS expects either a CT accept IU or a reject IU; MS received neither response, which violates the Fibre Channel Generic Services (FS-GS) specification.

Recommended Action

Check the integrity of the FC switch at the specified domain. It is not sending correct MS information as defined by the FC-FS standard.

Severity

ERROR

MS-1006

Message

```
<timestamp>, [MS-1006], <sequence-number>,, ERROR, <system-name>,  
MS Unexpected iu_data_sz=<number of bytes>
```

Probable Cause

Indicates that MS received IU data of unexpected size. The IU payload and the IU size might be inconsistent with each other or with the command that is currently being processed. This message is often transitory.

Recommended Action

Wait a few minutes and try the operation again.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

MS-1008

Message

```
<timestamp>, [MS-1008], <sequence-number>,, ERROR, <system-name>,  
MS Failure while initializing <action>
```

Probable Cause

MS failed while initializing the specified *action*. This message is often transitory.

The following *actions* might be displayed:

- <while writing to ms_els_q>
MS is unable to write a message to the MS Extended Link Service Queue.
- <while inserting timer to timer list>
MS is unable to add a timer to a resource.

Recommended Action

Wait a few minutes and try the operation again.

If the error persists, check the available memory on the switch using **memShow**.

Severity

ERROR

MS-1021

Message

```
<timestamp>, [MS-1021], <sequence-number>,, ERROR, <system-name>,  
MS WARMBOOT failure(FSS_MS_WARMINIT failed. Reason=<failure  
reason>)
```

Probable Cause

Indicates that the FSS warm recovery failed during WARM INIT phase of a reboot.

Recommended Action

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

NBFS Error Messages

NBFS-1001

Message

```
<timestamp>, [NBFS-1001], <sequence-number>,, INFO, <system-name>,  
Duplicate E_Port SCN from port <portnumber> in state <state change  
name> (<state change number>)
```

Probable Cause

Indicates that a duplicate E_Port State Change Number was reported. The neighbor finite state machine (NBFSM) states are as follows:

- 0 - Down
- 1 - Init
- 2 - Database Exchange
- 3 - Database Acknowledge Wait
- 4 - Database Wait
- 5 - Full

Recommended Action

No action is required.

Severity

INFO

NBFS-1002

Message

```
<timestamp>, [NBFS-1002], <sequence-number>,, ERROR, <system-name>,  
Wrong input: <state name> to neighbor FSM, state <current state  
name>, port <portnumber>
```

Probable Cause

Indicates that the wrong input was sent to the neighbor finite state machine (NBFSM). NBFSM states are as follows:

- 0 - Down
- 1 - Init
- 2 - Database Exchange
- 3 - Database Acknowledge Wait
- 4 - Database Wait
- 5 - Full

If this error occurs repeatedly, it means the protocol implementation between two connected switches has problems.

Recommended Action

Run the **nbrStateShow** command to check the neighbor state of the port listed in the message. If it is FULL, then this message can safely be ignored. Otherwise, run the **portDisable** and **portEnable** commands to refresh the port.

Severity

ERROR

NBFS-1003

Message

```
<timestamp>, [NBFS-1003], <sequence-number>,, WARNING,  
<system-name>, DB_XMIT_SET flag not set in state <current state  
name>, input <state name>, port <portnumber>
```

Probable Cause

Indicates that the database transmit set flag was not set for the specified input state on the specified port. Neighbor finite state machine (NBFSM) states are as follows:

- 0 - Down
- 1 - Init
- 2 - Database Exchange
- 3 - Database Acknowledge Wait
- 4 - Database Wait
- 5 - Full

Recommended Action

No action is required. The Fabric OS auto recovers from this problem.

Severity

WARNING

NS Error Messages

NS-1001

Message

```
<timestamp>, [NS-1001], <sequence-number>,, WARNING, <system-name>,  
The response for request 0x<CT command code> from remote switch  
0x<Domain Id> is larger than the max frame size the remote switch  
can support!
```

Probable Cause

Indicates that the response payload exceeds the maximum frame size the remote switch can handle.

Recommended Action

Run the **firmwareDownload** command to upgrade the remote switch with v4.3 or higher, or v3.2 or higher, as appropriate for the switch type, so that it can support GMI to handle frame fragmentation and reassembly.

You can also reduce the number of devices connected to the local switch.

Severity

WARNING

NS-1002

Message

```
<timestamp>, [NS-1002], <sequence-number>,, WARNING, <system-name>,  
Remote switch 0x<Domain Id> has firmware revision lower than 2.2:  
<Firmware Revision 1st character><Firmware Revision 2nd  
character><Firmware Revision 3rd character><Firmware Revision 4th  
character> which is not supported!
```

Probable Cause

Indicates that the local switch cannot interact with the remote switch due to incompatible or obsolete firmware.

Recommended Action

Run the **firmwareDownload** command to upgrade the remote switch to the latest level of firmware.

Severity

WARNING

NS-1003

Message

```
<timestamp>, [NS-1003], <sequence-number>,, INFO, <system-name>,  
Number of local devices <Current local device count>, exceeds the  
standby can support <Local device count that standby can support>,  
can't send update.
```

Probable Cause

Indicates that the name server on the standby CP has lower supported capability than the active CP due to different firmware versions running on the active and standby CPs. This means that the active and standby CPs are out of sync. Any execution of the **haFailover** or **firmwareDownload** commands will be disruptive.

Recommended Action

To avoid disruption of traffic in the event of an unplanned failover, schedule a **firmwareDownload** so that the active and standby CPs have the same firmware version.

Reduce the local device count to follow the capability of the lowest version of firmware.

Severity

INFO

NS-1004

Message

```
<timestamp>, [NS-1004], <sequence-number>,, INFO, <system-name>,  
Number of local devices <Current local device count>, exceeds the  
standby can support <Local device count that standby can support>,  
can't sync.
```

Probable Cause

Indicates that the name server on the standby CP has lower supported capability than the active CP due to different firmware versions running on the active and standby CPs. This means that the active and standby CPs are out of sync. Any execution of the **haFailover** or **firmwareDownload** commands will be disruptive.

Recommended Action

To avoid disruption of traffic in the event of an unplanned failover, schedule a **firmwareDownload** so that the active and standby CPs have the same firmware version.

Reduce the local device count to follow the capability of the lowest version of firmware.

Severity

INFO

PDM Error Messages

PDM-1001

Message

```
<timestamp>, [PDM-1001], <sequence-number>,, WARNING,  
<system-name>, Failed to parse the pdm config
```

Probable Cause

Indicates that the PDM process could not parse the configuration file. This might be caused by a missing configuration file during the installation.

Recommended Action

Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

PDM-1002

Message

```
<timestamp>, [PDM-1002], <sequence-number>,, WARNING,  
<system-name>, ipcInit failed
```

Probable Cause

Indicates that the PDM process could not initialize the IPC mechanism.

Recommended Action

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

PDM-1003

Message

```
<timestamp>, [PDM-1003], <sequence-number>,, WARNING,  
<system-name>, pdm [-d] -S <service> -s <instance>
```

Probable Cause

Indicates that a syntax error occurred when trying to launch the PDM process.

Recommended Action

Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

PDM-1004

Message

```
<timestamp>, [PDM-1004], <sequence-number>,, WARNING,  
<system-name>, Memory shortage
```

Probable Cause

Indicates that the PDM process ran out of memory.

Recommended Action

Reboot or power cycle the switch.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

PDM-1005

Message

```
<timestamp>, [PDM-1005], <sequence-number>,, WARNING,  
<system-name>, FSS register failed
```

Probable Cause

Indicates that the PDM failed to register to the FSS.

Recommended Action

Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

PDM-1006

Message

```
<timestamp>, [PDM-1006], <sequence-number>,, WARNING,  
<system-name>, Too many files in sync.conf
```

Probable Cause

Indicates that the configuration file *sync.conf* contains too many entries.

Recommended Action

Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

PDM-1007

Message

```
<timestamp>, [PDM-1007], <sequence-number>,, WARNING,  
<system-name>, File not created: <file name>
```

Probable Cause

Indicates that the PDM process failed to create the specified file name.

Recommended Action

Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

PDM-1008

Message

```
<timestamp>, [PDM-1008], <sequence-number>,, WARNING,  
<system-name>, Failed to get the number of uports
```

Probable Cause

Indicates that the PDM system call to *getcfg* failed.

Recommended Action

Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

PDM-1009

Message

```
<timestamp>, [PDM-1009], <sequence-number>,, WARNING,  
<system-name>, Can't update Port Config Data
```

Probable Cause

Indicates that the PDM system call to setcfg failed.

Recommended Action

Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

PDM-1010

Message

```
<timestamp>, [PDM-1010], <sequence-number>,, WARNING,  
<system-name>, File open failed: <file name>
```

Probable Cause

Indicates that the PDM process could not open the specified file name.

Recommended Action

Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

PDM-1011

Message

```
<timestamp>, [PDM-1011], <sequence-number>,, WARNING,  
<system-name>, File read failed: <file name>
```

Probable Cause

Indicates that the PDM process could not read data from the specified file name.

Recommended Action

Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

PDM-1012

Message

```
<timestamp>, [PDM-1012], <sequence-number>,, WARNING,  
<system-name>, File write failed: <file name>
```

Probable Cause

Indicates that the PDM process could not write data to the specified file name.

Recommended Action

Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

PDM-1013

Message

```
<timestamp>, [PDM-1013], <sequence-number>,, WARNING,  
<system-name>, File empty: <File Name>
```

Probable Cause

Indicates that the switch configuration file */etc/fabos/fabos.[0|1].conf* is empty.

Recommended Action

Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

PDM-1014

Message

```
<timestamp>, [PDM-1014], <sequence-number>,, WARNING,  
<system-name>, Access sysmod failed
```

Probable Cause

Indicates that a system call failed.

Recommended Action

Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

PDM-1017

Message

```
<timestamp>, [PDM-1017], <sequence-number>,, CRITICAL,  
<system-name>, System (<Error Code>): <Command>
```

Probable Cause

Indicates that a system call failed.

Recommended Action

Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

CRITICAL

PDM-1019

Message

```
<timestamp>, [PDM-1019], <sequence-number>,, WARNING,  
<system-name>, File path or trigger too long
```

Probable Cause

Indicates that one line of the *pdm.conf* file is too long.

Recommended Action

Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

PDM-1020

Message

```
<timestamp>, [PDM-1020], <sequence-number>,, WARNING,  
<system-name>, Long path name (<Path>/<File Name>), Skip
```

Probable Cause

Indicates that the indicated file path name is too long. The limit is 49 characters.

Recommended Action

Use short path name for the files to be replicated.

Severity

WARNING

PDM-1021

Message

```
<timestamp>, [PDM-1021], <sequence-number>,, WARNING,  
<system-name>, Failed to download area port map
```

Probable Cause

Indicates that a system call failed.

Recommended Action

Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

PDTR Error Messages

PDTR-1001

Message

```
<timestamp>, [PDTR-1001], <sequence-number>,, INFO, <system-name>,  
< informational message >
```

Probable Cause

Indicates that information has been written to the panic dump files. The watchdog register codes are as follows:

- 0x10000000 bit set means that the watch dog timer (WDT) forced a core reset.
- 0x20000000 bit set means that the WDT forced a chip reset.
- All other code values are reserved.

Recommended Action

Run the **pdShow** command to view the panic dump and core dump files.

Severity

INFO

PDTR-1002

Message

```
<timestamp>, [PDTR-1002], <sequence-number>,, INFO, <system-name>,  
< informational message >
```

Probable Cause

This message indicates that information has been written to the panic dump and core dump files and a trap generated. The watchdog register codes are as follows:

- 0x10000000 bit set means that the watch dog timer (WDT) forced a core reset.
- 0x20000000 bit set means that the WDT forced a chip reset.
- All other code values are reserved.

Recommended Action

Run the **pdShow** command to view the panic dump and core dump files.

Severity

INFO

PLAT Error Messages

PLAT-1000

Message

```
<timestamp>, [PLAT-1000], <sequence-number>,, CRITICAL,  
<system-name>, <Function name> <Error string>
```

Probable Cause

Indicates that nonrecoverable PCI errors have been detected.

Recommended Action

The system will be faulted and might automatically reboot.

If the system does not reboot, then try issuing a **reboot** command from a command-line prompt.

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

CRITICAL

PLAT-1001

Message

```
<timestamp>, [PLAT-1001], <sequence-number>,, INFO, <system-name>,  
Resetting standby CP (double reset may occur).
```

Probable Cause

Indicates that the standby CP is being reset. This message is typically generated by a CP that is in the process of becoming the active CP. Note that in certain circumstances a CP may experience a double reset and reboot twice in a row. A CP can recover automatically even if it has rebooted twice.

Recommended Action

No action is required.

Severity

INFO

PORT Error Messages

PORT-1003

Message

```
<timestamp>, [PORT-1003], <sequence-number>,, WARNING,  
<system-name>, Port <port number> Faulted because of many Link  
Failures
```

Probable Cause

Indicates that the specified port is now disabled because the link on this port had multiple failures that exceed an internally set threshold on the port. This problem is typically related to hardware.

Recommended Action

Check and replace (if necessary) the hardware attached to both ends of the specified *port number*, including:

- the media (SFPs)
- the cable (fiber optic or copper ISL)
- the attached devices

When finished checking the hardware, perform **portEnable** to reenable the port.

Severity

WARNING

PORT-1004

Message

```
<timestamp>, [PORT-1004], <sequence-number>,, INFO, <system-name>,  
Port <port number> could not be enabled because it is disabled due  
to long distance.
```

Probable Cause

Indicates that the specified port could not be enabled because other ports in the same port group have used up the buffers available for this port group. This most likely occurs because the other ports are configured as long distance.

Recommended Action

To enable this port, reconfigure the other E_Ports in the port group so they are either not long distance ports or not E_Ports. This will free up buffers and allow the port to be enabled.

Severity

INFO

PS Error Messages

PS-1000

Message

```
<timestamp>, [PS-1000], <sequence-number>,, CRITICAL,  
<system-name>, Failed to initialize Advanced Performance  
Monitoring.
```

Probable Cause

Indicates that an unexpected software error has occurred in Advanced Performance Monitoring. The Performance Monitor has failed to initialize.

Recommended Action

The CP should reboot (or fail over) automatically. If it does not, reboot or power cycle the switch to reinitiate the firmware.

Severity

CRITICAL

PS-1001

Message

```
<timestamp>, [PS-1001], <sequence-number>,, INFO, <system-name>,  
Advanced Performance Monitoring configuration updated due to change  
in PID format
```

Probable Cause

Indicates that the PID format was changed.

Recommended Action

No action is required. Refer to the *HP StorageWorks Fabric OS 5.x administrator guide* for more information about the PID format.

Severity

INFO

PS-1002

Message

```
<timestamp>, [PS-1002], <sequence-number>,, ERROR, <system-name>,  
Failed to initialize the tracing system for Advanced Performance  
Monitoring.
```

Probable Cause

Indicates that an unexpected software error has occurred in Advanced Performance Monitoring. The Performance Monitor tracing system has failed to initialize.

Recommended Action

Tracing will not be available for Advanced Performance Monitoring, but other functions should function normally. To retry activating tracing, reboot (or fail over) the CP.

Severity

ERROR

PS-1003

Message

```
<timestamp>, [PS-1003], <sequence-number>,, WARNING, <system-name>,  
Failed to set end-to-end monitoring mask on ISL ports.
```

Probable Cause

Indicates that the restoring configuration has attempted to set the end-to-end monitoring mask on at least one ISL port.

Recommended Action

No action is required. End-to-end monitoring is not supported on ISL ports when ISL monitoring is enabled. ISL monitoring can only be disabled through the Fabric Access API.

Severity

WARNING

PS-1004

Message

```
<timestamp>, [PS-1004], <sequence-number>,, WARNING, <system-name>,  
Failed to add end-to-end monitors on ISL ports.
```

Probable Cause

Indicates that the restoring configuration has attempted to add end-to-end monitors on at least one ISL port.

Recommended Action

No action is required. End-to-end monitoring is not supported on ISL ports when ISL monitoring is enabled. ISL monitoring can only be disabled through the Fabric Access API.

Severity

WARNING

PS-1005

Message

```
<timestamp>, [PS-1005], <sequence-number>,, WARNING, <system-name>,  
ISL monitor on port <port> stopped counting because no hardware  
resources are available
```

Probable Cause

Indicates that ISL and end-to-end monitors have used up all the hardware resources.

Recommended Action

To resume counting, delete some end-to-end monitors sharing the same hardware resource pool.

Severity

WARNING

PSWP Error Messages

PSWP-1001

Message

```
<timestamp>, [PSWP-1001], <sequence-number>,, INFO, <system-name>,  
Areas for port <wwn name corresponding to source port> and port <wwn  
name corresponding to destination port> are swapped. New area for  
port <wwn name corresponding to source port> is <wwn name  
corresponding to destination port> and port <new area corresponding  
to source wwn> is <new area corresponding to destination wwn>
```

Probable Cause

Indicates that the **portSwap** command has been issued by the user.

Recommended Action

No action is required.

Severity

INFO

PSWP-1002

Message

```
<timestamp>, [PSWP-1002], <sequence-number>,, INFO, <system-name>,  
Port Swap feature enabled
```

Probable Cause

Indicates that the **portSwap** feature has been enabled in the switch by the user.

Recommended Action

No action is required.

Severity

INFO

PSWP-1003

Message

```
<timestamp>, [PSWP-1003], <sequence-number>,, INFO, <system-name>,  
Port Swap feature disabled
```

Probable Cause

Indicates that the **portSwap** feature has been disabled in the switch by the user.

Recommended Action

No action is required.

Severity

INFO

PSWP-1004

Message

```
<timestamp>, [PSWP-1004], <sequence-number>,, WARNING,  
<system-name>, Port Swap configuration does not match Chassis  
configuration for switch <switch number>. Erasing port swap  
tables...
```

Probable Cause

Indicates that the **portSwap** configuration contradicts the chassis configuration.

Recommended Action

Redefine the port swap configuration so that it matches the chassis configuration.

Severity

WARNING

RCS Error Messages

RCS-1001

Message

```
<timestamp>, [RCS-1001], <sequence-number>,, INFO, <system-name>,  
RCS has been disabled. Some switches in the fabric do not support  
this feature
```

Probable Cause

Indicates that the RCS feature has been disabled on the local switch because not all switches in the fabric support RCS or the switch is in nonnative mode.

Recommended Action

Run the **rclInfoShow** command to view RCS capability on the fabric. RCS is supported in Fabric OS v2.6, v3.1 and greater, v4.1 and greater.

Run the **firmwareDownload** command to upgrade the firmware for any switches that do not support RCS.

Severity

INFO

RCS-1002

Message

```
<timestamp>, [RCS-1002], <sequence-number>,, INFO, <system-name>,  
RCS has been enabled.
```

Probable Cause

Indicates that the RCS feature has been enabled. RCS must be capable on all switches in the fabric to be enabled. If all switches are capable, it is automatically enabled.

Recommended Action

No action is required.

Severity

INFO

RCS-1003

Message

```
<timestamp>, [RCS-1003], <sequence-number>,, ERROR, <system-name>,  
Failed to allocate memory: (<function name>)
```

Probable Cause

Indicates that the specified RCS function failed to allocate memory.

Recommended Action

This message is usually transitory. Wait a few minutes and retry the command.

Check memory usage on the switch using the **memShow** command.

Reboot or power cycle the switch.

Severity

ERROR

RCS-1004

Message

```
<timestamp>, [RCS-1004], <sequence-number>,, ERROR, <system-name>,  
Application(<application name>) not registered.(<error string>)
```

Probable Cause

Indicates that a specified application did not register with RCS.

Recommended Action

Run the **haShow** command to view the HA state.

Run the **haDisable** and the **haEnable** commands.

Run the **rclInfoShow** command to view RCS capability on the fabric. RCS is supported in Fabric OS v2.6, v3.1 and greater, v4.1 and greater.

Run the **firmwareDownload** command to upgrade the firmware for any switches that do not support RCS.

Severity

ERROR

RCS-1005

Message

```
<timestamp>, [RCS-1005], <sequence-number>,, INFO, <system-name>,  
State <RCS phase>, Application <Application ID> returned 0x<Reject  
code>.
```

Probable Cause

Indicates that a receiving switch is rejecting an RCS phase.

Recommended Action

If the reject is in ACA phase, wait several minutes and then retry the operation from the sender switch.

If the reject is in the SFC phase, check if the application license exists for the local domain and if the application data is compatible.

Severity

INFO

RCS-1006

Message

```
<timestamp>, [RCS-1006], <sequence-number>,, INFO, <system-name>,  
State <RCS phase>, Application <Application ID>, RCS CM. Domain  
<Domain ID that sent the reject> returned 0x<Reject code>.
```

Probable Cause

Indicates that a remote domain rejected an RCS phase initiated by an application on the local switch.

- If the reject phase is ACA, the remote domain might be busy and could not process the new request.
- If the reject phase is SFC, the data sent by the application might not be compatible or the domain does not have the license to support that application.

Recommended Action

If the reject is in ACA phase, wait several minutes and then retry the operation.

If the reject is in the SFC phase, check if the application license exists for the remote domain and if the application data is compatible.

Severity

INFO

RCS-1007

Message

```
<timestamp>, [RCS-1007], <sequence-number>,, ERROR, <system-name>,  
Cannot propagate new Zone DB as it exceeds domain <domain number>'s  
maximum supported Zone DB size. Retry after reducing Zone DB size to  
<max zone db size>.
```

Probable Cause

Indicates that a switch in the fabric does not support the current size of the zone database. The `<max zone db size>` variable displays the maximum size of the zone database this switch can accept.

Recommended Action

Reduce the zone database size.

Severity

ERROR

RCS-1008

Message

```
<timestamp>, [RCS-1008], <sequence-number>,, ERROR, <system-name>,  
Domain <domain number> Lowest Max Zone DB size
```

Probable Cause

Indicates that switch specified has the lowest maximum zone database size in the fabric.

Recommended Action

Reduce the zone database size.

Severity

ERROR

RPCD Error Messages

RPCD-1001

Message

```
<timestamp>, [RPCD-1001], <sequence-number>,, WARNING,  
<system-name>, Authentication Error: client \"<IP address>\" has  
bad credentials: <bad user name and password pair>
```

Probable Cause

Indicates that an authentication error was reported. The specified *client IP address* has faulty credentials.

Recommended Action

Enter the correct user name and password from the Fabric Access API host.

Severity

WARNING

RPCD-1002

Message

```
<timestamp>, [RPCD-1002], <sequence-number>,, WARNING,  
<system-name>, Missing certificate file. Secure RPCd is disabled.
```

Probable Cause

Indicates that an SSL certificate is missing.

Recommended Action

To enable RPCD in secure mode, install a valid SSL certificate on the switch.

Severity

WARNING

RPCD-1003

Message

```
<timestamp>, [RPCD-1003], <sequence-number>,, WARNING,  
<system-name>, Permission denied accessing certificate file. Secure  
RPCd is disabled.
```

Probable Cause

Indicates that the SSL certificate file configured on the switch could not be accessed because root did not have read access.

Recommended Action

Change the file system access level for the certificate file to have root read-level access.

Severity

WARNING

RPCD-1004

Message

```
<timestamp>, [RPCD-1004], <sequence-number>,, WARNING,  
<system-name>, Invalid certificate file. Secure RPCd is disabled.
```

Probable Cause

Indicates that the SSL certificate file has been corrupted.

Recommended Action

To enable RPCD in secure mode, install a valid SSL certificate on the switch.

Severity

WARNING

RPCD-1005

Message

```
<timestamp>, [RPCD-1005], <sequence-number>,, WARNING,  
<system-name>, Missing private key file. Secure RPCd is disabled.
```

Probable Cause

Indicates that the private key file is missing.

Recommended Action

Run the **pkiCreate** command to install a valid private key file.

Severity

WARNING

RPCD-1006

Message

```
<timestamp>, [RPCD-1006], <sequence-number>,, WARNING,  
<system-name>, Permission denied accessing private key file. Secure  
RPCd is disabled.
```

Probable Cause

Indicates that the private key file configured on the switch could not be accessed because root did not have read access.

Recommended Action

Change the file system access level for the private key file to have root read-level access.

Severity

WARNING

RPCD-1007

Message

```
<timestamp>, [RPCD-1007], <sequence-number>,, WARNING,  
<system-name>, Invalid private file. Secure RPCd is disabled.
```

Probable Cause

Indicates that the private key file has been corrupted.

Recommended Action

Run the **pkiCreate** command to install a valid private key file.

Severity

WARNING

RTWR Error Messages

RTWR-1001

Message

```
<timestamp>, [RTWR-1001], <sequence-number>,, ERROR, <system-name>,  
RTWR <routine: error message> 0x<detail 1>, 0x<detail 2>, 0x<detail  
3>, 0x<detail 4>, 0x<detail 5>
```

Probable Cause

Indicates that an error occurred in the RTWR. The message provides the name of the routine having the error, and more specific error information. The values in details 1 through 5 might provide more information.

Recommended Action

No action is required.

Severity

ERROR

RTWR-1002

Message

```
<timestamp>, [RTWR-1002], <sequence-number>,, WARNING,  
<system-name>, RTWR <error message> 0x<detail1>, 0x<detail2>,  
0x<detail3>, 0x<detail4>, 0x<detail5>
```

Probable Cause

Indicates that the RTWR has exhausted the maximum number of retries sending data to the specified domain. Details are as follows:

- RTWRTransmit: Max retries exhausted
- detail1: Port
- detail2: Domain
- detail3: Retry Count
- detail4: Status
- detail5: Process ID

Recommended Action

Run the **fabricShow** command to see if the specified domain ID is online.

Enable the switch with the specified domain ID.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

RTWR-1003

Message

```
<timestamp>, [RTWR-1003], <sequence-number>,, INFO, <system-name>,  
<module name>: RTWR retry <number of times retried> to domain  
<domain ID>, iu_data <first word of iu_data>
```

Probable Cause

Indicates how many times RTWR failed to get a response and retried.

Recommended Action

Run the **dom** command to verify that the specified domain ID is reachable.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

INFO

SCN Error Messages

SCN-1001

Message

```
<timestamp>, [SCN-1001], <sequence-number>,, CRITICAL,  
<system-name>, SCN queue overflow for process <daemon name>
```

Probable Cause

Indicates that an attempt to write an SCN (state change notification) message to a specific queue has failed because the SCN queue for the specified *daemon name* is full. This might be caused by the daemon hanging or if the system is busy.

The valid values for *daemon name* are:

- fabricd
- asd
- evmd
- fcpd
- webd
- msd
- nsd
- psd
- snmpd
- zoned
- fspf
- tsd

Recommended Action

If this message is caused by the system being busy, the condition is temporary.

If this message is caused by a hung daemon, the software watchdog will cause the daemon to dump the core and reboot the switch. In this case, run the **saveCore** command to send the core files using FTP to a secure server location.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

CRITICAL

SEC Error Messages

SEC-1001

Message

```
<timestamp>, [SEC-1001], <sequence-number>,, ERROR, <system-name>,  
RCS process fails: <Reason text>
```

Probable Cause

Indicates that the RCS (reliable commit service) process fails to complete. RCS is a reliable mechanism to transfer data from one switch to other switches within the fabric. This mechanism guarantees that either all

switches commit to the new database or none of them update to the new database. This process can fail if one switch in the fabric is busy or in an error state that cannot accept the database.

Recommended Action

RCS is used when the security database is changed by a command run by security (for example, **secPolicySave**, **secPolicyActivate**, or **secVersionReset**). If the switch is busy, the command might fail the first time only; retry after the first fail.

Run the **rcsInfoShow** command to view RCS capability on the fabric. RCS must be capable on all switches in the fabric to be enabled. If all switches are capable, it is automatically enabled.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

SEC-1002

Message

```
<timestamp>, [SEC-1002], <sequence-number>,, ERROR, <system-name>,  
Security data fails: <Reason Text>
```

Probable Cause

Indicates that the receiving switch fails to validate the security database sent from the primary FCS switch. This could result from the data package being corrupted, the time stamp on the package is out of range as a result of replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure might be due to an internal error, such as losing the primary public key or an invalid database.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that switch. The error might also be a result of an internal corruption or a hacker attack to the secure fabric.

Severity

ERROR

SEC-1003

Message

```
<timestamp>, [SEC-1003], <sequence-number>,, WARNING,  
<system-name>, Fail to download security data to domain <Domain  
number> after <Number of retries> retries
```

Probable Cause

Indicates that the specified domain number failed to download security data after the specified number of attempts. The primary switch will segment the failed switch after 30 tries. The failed switch might have had some internal error and failed to accept the database download.

Recommended Action

Reset the version stamp on the switch to 0 using the **secVersionReset** command and then rejoin the switch to the fabric.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

SEC-1005

Message

```
<timestamp>, [SEC-1005], <sequence-number>,, INFO, <system-name>,  
Primary FCS receives data request from domain <Domain number>
```

Probable Cause

Indicates that the primary FCS received a data request from the specified domain. For example, if the switch fails to update the database or is attacked (data injection), a message is generated to the primary FCS to try to correct and resync with the rest of the switches in the fabric.

Recommended Action

Check the fabric status, using **secFabricShow** to verify that the fabric is not being attacked by unauthorized users.

Severity

INFO

SEC-1006

Message

```
<timestamp>, [SEC-1006], <sequence-number>,, WARNING,  
<system-name>, Security statistics error: Failed to reset due to  
invalid <data>.
```

Probable Cause

Indicates that invalid data has been received for any statistic-related command for security (**secStatsShow** or **secStatsReset**). The counter is updated automatically when a security violation occurs. This message might also occur if the updating counter fails.

Recommended Action

If the message is the result of a user command, retry the statistic command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

SEC-1007

Message

```
<timestamp>, [SEC-1007], <sequence-number>,, INFO, <system-name>,  
Security violation: Unauthorized host with IP address <IP address  
of the violating host> tries to establish API connection.
```

Probable Cause

Indicates that a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended Action

Check for unauthorized access to the switch through the API connection.

Severity

INFO

SEC-1008

Message

```
<timestamp>, [SEC-1008], <sequence-number>,, INFO, <system-name>,  
Security violation: Unauthorized host with IP address <IP address  
of the violating host> tries to establish HTTP connection.
```

Probable Cause

Indicates that a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended Action

Check for unauthorized access to the switch through the HTTP connection.

Severity

INFO

SEC-1009

Message

```
<timestamp>, [SEC-1009], <sequence-number>,, INFO, <system-name>,  
Security violation: Unauthorized host with IP address <IP address  
of the violating host> tries to establish TELNET connection.
```

Probable Cause

Indicates that a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended Action

Check for unauthorized access to the switch through the telnet connection.

Severity

INFO

SEC-1016

Message

```
<timestamp>, [SEC-1016], <sequence-number>,, INFO, <system-name>,  
Security violation: Unauthorized host with IP address <IP address  
of the violating host> tries to establish SSH connection.
```

Probable Cause

Indicates that a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended Action

Check for unauthorized access to the switch through the SSH connection.

Severity

INFO

SEC-1022

Message

```
<timestamp>, [SEC-1022], <sequence-number>,, WARNING,  
<system-name>, Failed to <operation> PKI objects.
```

Probable Cause

Indicates that the security server failed to generate or validate either the public or private key pair or the CSR.

Recommended Action

Run the **pkiShow** command and verify that all PKI objects exist on the switch. If the private key does not exist, follow the steps for re-creating PKI objects, outlined in the Secure Fabric OS User's Guide. If a certificate does not exist or is invalid, install the certificate by following the field upgrade process.

Severity

WARNING

SEC-1024

Message

```
<timestamp>, [SEC-1024], <sequence-number>,, INFO, <system-name>,  
The <DB name> security database is too large to fit in flash.
```

Probable Cause

Indicates that the size of the security database is too large for the flash memory. The size of the security database increases with the number of entries in each policy.

Recommended Action

Reduce the size of the security database by reducing the number of entries within each policy.

Severity

INFO

SEC-1025

Message

```
<timestamp>, [SEC-1025], <sequence-number>,, ERROR, <system-name>,  
Invalid IP <IP address>.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1026

Message

```
<timestamp>, [SEC-1026], <sequence-number>,, ERROR, <system-name>,  
Not a valid format [<switch member ID>] for switch member.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1028

Message

```
<timestamp>, [SEC-1028], <sequence-number>,, ERROR, <system-name>,  
No name is specified.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1029

Message

```
<timestamp>, [SEC-1029], <sequence-number>,, ERROR, <system-name>,  
Invalid character in <policy name>.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1030

Message

```
<timestamp>, [SEC-1030], <sequence-number>,, ERROR, <system-name>,  
The length of the name invalid.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1031

Message

```
<timestamp>, [SEC-1031], <sequence-number>,, WARNING,  
<system-name>, Current security policy DB cannot be supported by  
standby. CPs will go out of sync.
```

Probable Cause

The security database size is not supported by the standby CP.

Recommended Action

Reduce the database size by reducing the security policy size.

Severity

WARNING

SEC-1032

Message

```
<timestamp>, [SEC-1032], <sequence-number>,, ERROR, <system-name>,  
Empty FCS list is not allowed.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1033

Message

```
<timestamp>, [SEC-1033], <sequence-number>,, ERROR, <system-name>,  
The * symbol is only used to create the policy. Command terminated
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1034

Message

```
<timestamp>, [SEC-1034], <sequence-number>,, ERROR, <system-name>,  
Invalid member <policy member>.
```

Probable Cause

Indicates that the input list has an invalid member.

Recommended Action

Verify your member names, and input the correct information.

Severity

ERROR

SEC-1035

Message

```
<timestamp>, [SEC-1035], <sequence-number>,, ERROR, <system-name>,  
Invalid device WWN <Device WWN>.
```

Probable Cause

Indicates that the specified WWN is invalid.

Recommended Action

Enter the correct WWN value.

Severity

ERROR

SEC-1036

Message

```
<timestamp>, [SEC-1036], <sequence-number>,, ERROR, <system-name>,  
Invalid device name <device name>. Missing colon
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1037

Message

```
<timestamp>, [SEC-1037], <sequence-number>,, ERROR, <system-name>,  
Invalid WWN format <Invalid WWN>.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1038

Message

```
<timestamp>, [SEC-1038], <sequence-number>,, ERROR, <system-name>,  
Invalid domain <Domain ID>.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1040

Message

```
<timestamp>, [SEC-1040], <sequence-number>,, ERROR, <system-name>,  
Invalid portlist (<port list>). Cannot combine * with port member in  
the same portlist.
```

Probable Cause

Indicates that the port list contains the wildcard asterisk (*) character.

Recommended Action

You cannot use the asterisk in a port list. Enter the port list values without any wildcards.

Severity

ERROR

SEC-1041

Message

```
<timestamp>, [SEC-1041], <sequence-number>,, ERROR, <system-name>,  
Invalid port member <port member> in portlist (<port list>).  
<Reason>.
```

Probable Cause

Indicates that the port member is invalid for one of the following reasons:

- The value is not a number.
- The value is too long. Valid numbers must be between one and three characters long.
- The value cannot be parsed due to invalid characters.

Recommended Action

Use valid syntax when entering port members.

Severity

ERROR

SEC-1042

Message

```
<timestamp>, [SEC-1042], <sequence-number>,, ERROR, <system-name>,  
Invalid area member <port member> in portlist (<Port list>). Out of  
range (<Minimum value> - <Maximum value>).
```

Probable Cause

Indicates that the specified area member is not within the minimum and maximum values.

Recommended Action

Use valid syntax when entering area numbers.

Severity

ERROR

SEC-1043

Message

```
<timestamp>, [SEC-1043], <sequence-number>,, ERROR, <system-name>,  
Invalid port range <Minimum> - <Maximum>.
```

Probable Cause

Indicates that the specified port is not within the minimum and maximum range.

Recommended Action

Use valid syntax when entering port ranges.

Severity

ERROR

SEC-1044

Message

```
<timestamp>, [SEC-1044], <sequence-number>,, ERROR, <system-name>,  
Duplicate member <member ID> in (<List>).
```

Probable Cause

Indicates that the specified member is a duplicate in the input list. The list can be a policy list or a switch member list.

Recommended Action

Do not specify any duplicates.

Severity

ERROR

SEC-1045

Message

```
<timestamp>, [SEC-1045], <sequence-number>,, ERROR, <system-name>,  
Too many port members.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1046

Message

```
<timestamp>, [SEC-1046], <sequence-number>,, ERROR, <system-name>,  
Empty list.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1049

Message

```
<timestamp>, [SEC-1049], <sequence-number>,, ERROR, <system-name>,  
Invalid switch name <switch name>.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1050

Message

```
<timestamp>, [SEC-1050], <sequence-number>,, ERROR, <system-name>,  
There are more than one switches with the same name <switch name> in  
the fabric.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1051

Message

```
<timestamp>, [SEC-1051], <sequence-number>,, ERROR, <system-name>,  
Missing brace for port list <port list>.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1052

Message

```
<timestamp>, [SEC-1052], <sequence-number>,, ERROR, <system-name>,  
Invalid input.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1053

Message

```
<timestamp>, [SEC-1053], <sequence-number>,, ERROR, <system-name>,  
Invalid pFCS list <pFCS list>
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1054

Message

```
<timestamp>, [SEC-1054], <sequence-number>,, ERROR, <system-name>,  
Invalid FCS list length <list length>
```


Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1055

Message

```
<timestamp>, [SEC-1055], <sequence-number>,, ERROR, <system-name>,  
Invalid FCS list <WWN list>
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1056

Message

```
<timestamp>, [SEC-1056], <sequence-number>,, ERROR, <system-name>,  
Invalid postion <New position>. Only <Number of members in FCS list>  
members in list.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1057

Message

```
<timestamp>, [SEC-1057], <sequence-number>,, ERROR, <system-name>,  
No change. Both positions are the same.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1059

Message

```
<timestamp>, [SEC-1059], <sequence-number>,, ERROR, <system-name>,  
Fail to <operation, e.g., save, delete, etc.,> <named item> to  
flash.
```

Probable Cause

Indicates that the operation failed when writing to flash.

Recommended Action

Run the **saveCore** command to FTP files from the switch and remove them from the flash.

Severity

ERROR

SEC-1062

Message

```
<timestamp>, [SEC-1062], <sequence-number>,, ERROR, <system-name>,  
Invalid number of Domains in Domain List.
```

Probable Cause

Indicates either that no domains or domains more than the maximum are specified.

Recommended Action

Enter the correct number of domains.

Severity

ERROR

SEC-1063

Message

```
<timestamp>, [SEC-1063], <sequence-number>,, ERROR, <system-name>,  
Failed to reset statistics.
```

Probable Cause

Indicates that either the type or the domains specified are invalid.

Recommended Action

Enter valid input.

Severity

ERROR

SEC-1064

Message

```
<timestamp>, [SEC-1064], <sequence-number>,, ERROR, <system-name>,  
Failed to sign message.
```

Probable Cause

Indicates that the PKI objects on the switch are not in a valid state and the signature operation failed.

Recommended Action

Run the **pkiShow** command to verify that all PKI objects are valid. If PKI objects are not valid, generate the PKI objects and install the certificate by following the field upgrade process.

Severity

ERROR

SEC-1065

Message

```
<timestamp>, [SEC-1065], <sequence-number>,, ERROR, <system-name>,  
Invalid character in list.
```

Probable Cause

Indicates that the input list has an invalid character.

Recommended Action

Enter valid input.

Severity

ERROR

SEC-1069

Message

```
<timestamp>, [SEC-1069], <sequence-number>,, ERROR, <system-name>,  
Security Database is corrupted.
```

Probable Cause

Indicates that the security database is corrupted for unknown reasons.

Recommended Action

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

SEC-1071

Message

```
<timestamp>, [SEC-1071], <sequence-number>,, ERROR, <system-name>,  
No new data to apply.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1072

Message

```
<timestamp>, [SEC-1072], <sequence-number>,, ERROR, <system-name>,  
<Policy type> Policy List is Empty!
```

Probable Cause

Indicates that the specific policy type is empty. The security database is corrupted for unknown reasons.

Recommended Action

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

SEC-1073

Message

```
<timestamp>, [SEC-1073], <sequence-number>,, ERROR, <system-name>,  
No FCS policy in list!
```

Probable Cause

Indicates that the specific policy type is empty. The security database is corrupted for unknown reasons.

Recommended Action

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

SEC-1074

Message

```
<timestamp>, [SEC-1074], <sequence-number>,, ERROR, <system-name>,  
Cannot execute the command on this switch. Please check the secure  
mode and FCS status.
```

Probable Cause

Indicates that a security command was run on a switch that is not allowed to run it either because it is in non-secure mode or because it does not have required FCS privilege.

Recommended Action

If a security operation that is not allowed in non-secure mode is attempted, do not perform the operation in non-secure mode. In secure mode, run the command from a switch that has required privilege, that is, either a backup FCS or primary FCS.

Severity

ERROR

SEC-1075

Message

```
<timestamp>, [SEC-1075], <sequence-number>,, ERROR, <system-name>,  
Fail to <operation> new policy set on all switches.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1076

Message

```
<timestamp>, [SEC-1076], <sequence-number>,, ERROR, <system-name>,  
NoNodeWWNZoning option has been changed.
```

Probable Cause

Indicates that the NoNodeWWNZoning option has been changed. If the option is turned on, a zone member can be added using node WWNs, but the member will not be able to communicate with others nodes in the zone.

Recommended Action

Reenable the current zone configuration for the change to take effect.

Severity

ERROR

SEC-1077

Message

```
<timestamp>, [SEC-1077], <sequence-number>,, ERROR, <system-name>,  
Failed to activate new policy set on all switches.
```

Probable Cause

Indicates that the policy could not be activated. Reasons can be no memory, switch busy, and so on.

Recommended Action

Run the **secFabricShow** command to verify that all switches in the fabric are in the ready state. Retry the command when all switches are ready.

Severity

ERROR

SEC-1078

Message

```
<timestamp>, [SEC-1078], <sequence-number>,, ERROR, <system-name>,  
No new data to abort.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1079

Message

```
<timestamp>, [SEC-1079], <sequence-number>,, ERROR, <system-name>,  
Invalid policy name <Policy name>.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1080

Message

```
<timestamp>, [SEC-1080], <sequence-number>,, ERROR, <system-name>,  
Operation denied. Please, use secModeEnable command.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1081

Message

```
<timestamp>, [SEC-1081], <sequence-number>,, ERROR, <system-name>,  
DCC_POLICY is not allowed without a unique identifier.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1082

Message

```
<timestamp>, [SEC-1082], <sequence-number>,, ERROR, <system-name>,  
Failed to create <policy name> policy.
```

Probable Cause

Indicates that the security policy was not created due to faulty input or low resources.

Recommended Action

Use proper syntax when creating policies. If the security database is too large, you must delete other members within the database before adding new members to a policy.

Severity

ERROR

SEC-1083

Message

```
<timestamp>, [SEC-1083], <sequence-number>,, ERROR, <system-name>,  
Name already exists.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1084

Message

```
<timestamp>, [SEC-1084], <sequence-number>,, ERROR, <system-name>,  
Name exists for different type <Policy name>.
```

Probable Cause

Indicates that the specified policy already exists.

Recommended Action

No action is required.

Severity

ERROR

SEC-1085

Message

```
<timestamp>, [SEC-1085], <sequence-number>,, ERROR, <system-name>,  
Failed to create <Policy name>.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1086

Message

```
<timestamp>, [SEC-1086], <sequence-number>,, ERROR, <system-name>,  
The security database is too large to fit in flash.
```

Probable Cause

Indicates that the security database has more data than the flash can accommodate.

Recommended Action

Reduce the number of entries in some policies to decrease the security database size.

Severity

ERROR

SEC-1088

Message

```
<timestamp>, [SEC-1088], <sequence-number>,, ERROR, <system-name>,  
Cannot execute the command. Please try later.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1089

Message

```
<timestamp>, [SEC-1089], <sequence-number>,, ERROR, <system-name>,  
Policy name <Policy name> not found. Please, use secPolicyCreate.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1090

Message

```
<timestamp>, [SEC-1090], <sequence-number>,, ERROR, <system-name>,  
SCC list contains FCS member. Please remove member from the FCS  
policy first.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1091

Message

```
<timestamp>, [SEC-1091], <sequence-number>,, ERROR, <system-name>,  
No policy to remove.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1092

Message

```
<timestamp>, [SEC-1092], <sequence-number>,, ERROR, <system-name>,  
<Policy name> Name not found.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1093

Message

```
<timestamp>, [SEC-1093], <sequence-number>,, ERROR, <system-name>,  
New FCS list must have at least one member in common with current  
FCS list.
```

Probable Cause

Indicates that the new FCS list does not have a common member with the existing FCS list.

Recommended Action

Resubmit the command with at least one member of the new FCS list in common with the current FCS list.

Severity

ERROR

SEC-1094

Message

```
<timestamp>, [SEC-1094], <sequence-number>,, ERROR, <system-name>,  
Policy member not found.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1095

Message

```
<timestamp>, [SEC-1095], <sequence-number>,, ERROR, <system-name>,  
Deleting FCS policy is not allowed.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1096

Message

```
<timestamp>, [SEC-1096], <sequence-number>,, ERROR, <system-name>,  
Failed to delete <Policy name>. <Reason text>
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1097

Message

```
<timestamp>, [SEC-1097], <sequence-number>,, ERROR, <system-name>,  
Cannot find <active or defined> policy set.
```

Probable Cause

Indicates that the specified policy could not be found.

Recommended Action

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

SEC-1098

Message

```
<timestamp>, [SEC-1098], <sequence-number>,, ERROR, <system-name>,  
No <active or defined> FCS list.
```

Probable Cause

Indicates that the specified policy could not be found.

Recommended Action

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

SEC-1099

Message

```
<timestamp>, [SEC-1099], <sequence-number>,, ERROR, <system-name>,  
Please enable your switch before running secModeEnable.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1100

Message

```
<timestamp>, [SEC-1100], <sequence-number>,, ERROR, <system-name>,  
FCS switch present. Command terminated.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1101

Message

```
<timestamp>, [SEC-1101], <sequence-number>,, ERROR, <system-name>,  
Failed to enable security on all switches. Please retry later.
```

Probable Cause

Indicates that the security enable failed on the fabric because one or more switches in the fabric are busy.

Recommended Action

Verify that the security event was planned. If the security event was planned, run the **secFabricShow** command to verify that all switches in the fabric are in the ready state. When all switches are in the ready state, retry the operation.

Severity

ERROR

SEC-1102

Message

```
<timestamp>, [SEC-1102], <sequence-number>,, ERROR, <system-name>,  
Fail to download <security data>.
```

Probable Cause

Indicates that the switch failed to download certificate, security database, or policies. This can happen when switch does not get enough resources to complete the operation, fabric has not stabilized, or policy database is an invalid format.

Recommended Action

Wait for fabric to become stable and then retry the operation. If the policy database is in an illegal format (with **configDownload**), correct the format and retry the operation.

Severity

ERROR

SEC-1104

Message

```
<timestamp>, [SEC-1104], <sequence-number>,, ERROR, <system-name>,  
Fail to get primary <Certificate or public key>.
```

Probable Cause

Indicates that the switch failed to get either the primary certificate or a primary public key.

Recommended Action

Verify that the primary switch has a valid certificate installed and retry the operation. If a valid certificate is not installed, install a certificate by following the procedure specified in the *Secure Fabric OS User's Guide*.

Severity

ERROR

SEC-1105

Message

```
<timestamp>, [SEC-1105], <sequence-number>,, ERROR, <system-name>,  
Fail to disable secure mode on all switches.
```

Probable Cause

Indicates that the switch failed to disable security in the fabric. This could happen if the switch cannot get the required resources to complete the command, and sending to a remote domain fails or the remote domain returns an error.

Recommended Action

Run the **secFabricShow** to verify that all switches in the fabric are in the ready state. Retry the command when all switches are READY.

Severity

ERROR

SEC-1106

Message

```
<timestamp>, [SEC-1106], <sequence-number>,, ERROR, <system-name>,  
Failed to sign message data.
```

Probable Cause

Indicates that some PKI objects on the switch are not in a valid state, and a signature operation failed.

Recommended Action

Run the **pkiShow** command and verify that all PKI objects exist on the switch. If a failure to validate PKI objects occurs, follow the steps for re-creating PKI objects outlined in the *Secure Fabric OS User's Guide*.

Severity

ERROR

SEC-1107

Message

```
<timestamp>, [SEC-1107], <sequence-number>,, INFO, <system-name>,  
Stamp is 0.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

INFO

SEC-1108

Message

```
<timestamp>, [SEC-1108], <sequence-number>,, ERROR, <system-name>,  
Fail to reset stamp on all switches.
```

Probable Cause

Indicates that a version reset operation failed either because the switch could not get all the required resources to perform the operation or because it failed to send the message to all switches in the fabric.

Recommended Action

Verify that the security event was planned. If the security event was planned, run the **secFabricShow** command to verify that all switches in the fabric are in the ready state. When all switches are in the ready state, retry the operation.

Severity

ERROR

SEC-1110

Message

```
<timestamp>, [SEC-1110], <sequence-number>,, ERROR, <system-name>,  
FCS list must be the first entry in the [Defined Security policies]  
section. Fail to download defined database.
```

Probable Cause

Indicates that a security policy download is attempted with a defined policy that does not have the FCS policy as the first policy. The FCS policy is required to be the first policy in the defined security database.

Recommended Action

Download a correct configuration with the FCS policy as the first policy in the defined security database.

Severity

ERROR

SEC-1111

Message

```
<timestamp>, [SEC-1111], <sequence-number>,, ERROR, <system-name>,  
New defined FCS list must have at least one member in common with  
current active FCS list. Fail to download defined database.
```

Probable Cause

Indicates that the defined and active FCS policy list failed to have at least one member in common.

Recommended Action

A new FCS policy list must have at least one member in common with the previous FCS policy.

Severity

ERROR

SEC-1112

Message

```
<timestamp>, [SEC-1112], <sequence-number>,, ERROR, <system-name>,  
FCS list must be the first entry in the Active Security policies,  
and the same as the current active FCS list in the switch.
```

Probable Cause

Indicates that either a security policy download is attempted with an active policy that does not have the FCS policy as the first policy or the FCS policy is not same as the current FCS policy on the switch.

Recommended Action

Make sure that the new FCS policy is the same as the current FCS policy on the switch.

Severity

ERROR

SEC-1115

Message

```
<timestamp>, [SEC-1115], <sequence-number>,, ERROR, <system-name>,  
No primary FCS to failover.
```

Probable Cause

Indicates that during an attempted **secFcsFailover**, no primary FCS is present in the fabric.

Recommended Action

Run the **secFabricShow** command to verify that all switches in fabric are in the ready state. When all switches are in the ready state, retry the operation.

Severity

ERROR

SEC-1116

Message

```
<timestamp>, [SEC-1116], <sequence-number>,, ERROR, <system-name>,  
Fail to commit failover.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1117

Message

```
<timestamp>, [SEC-1117], <sequence-number>,, INFO, <system-name>,  
Fail to set <data>.
```

Probable Cause

Indicates that the switch failed to save the data received by the primary FCS switch. This data can be an FCS password, a non-FCS password, SNMP data, or multiple user authentication data.

Recommended Action

Run the **secFabricShow** command to verify that all switches in fabric are in the ready state. When all switches are in the ready state, retry the operation.

Severity

INFO

SEC-1118

Message

```
<timestamp>, [SEC-1118], <sequence-number>,, INFO, <system-name>,  
Fail to set SNMP string.
```

Probable Cause

Indicates that the SNMP string could not be set.

Recommended Action

Usually this problem is transient. Retry the command.

Severity

INFO

SEC-1119

Message

```
<timestamp>, [SEC-1119], <sequence-number>,, INFO, <system-name>,  
Secure mode has been enabled.
```

Probable Cause

Indicates that the secure Fabric OS was enabled by the **secModeEnable** command.

Recommended Action

Verify that the security event was planned. If the security event was planned, there is no action required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-1121

Message

```
<timestamp>, [SEC-1121], <sequence-number>,, ERROR, <system-name>,  
Time is out of range when <text>.
```

Probable Cause

Indicates that the time on the switch is not synchronized with the primary FCS, the data packet is corrupted, or a replay attack is launched on the switch.

Recommended Action

Verify that the security event was planned. If the security event was planned, verify that all switches in the fabric are in time synchronization with the primary FCS and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

Severity

ERROR

SEC-1122

Message

```
<timestamp>, [SEC-1122], <sequence-number>,, INFO, <system-name>,  
Error code: <Domain ID>, <Error message>.
```

Probable Cause

Indicates that one of the switches in the fabric could not communicate with the primary FCS.

Recommended Action

Run the **secFabricShow** command to verify that all switches in fabric are in the ready state. When all switches are in the ready state, retry the operation.

Severity

INFO

SEC-1123

Message

```
<timestamp>, [SEC-1123], <sequence-number>,, INFO, <system-name>,  
Security database downloaded by Primary FCS.
```

Probable Cause

Indicates that the security database was successfully downloaded from the primary FCS.

Recommended Action

No action is required.

Severity

INFO

SEC-1124

Message

```
<timestamp>, [SEC-1124], <sequence-number>,, INFO, <system-name>,  
Secure Mode is off.
```

Probable Cause

Indicates that a secure mode disable is attempted in a non-secure fabric.

Recommended Action

No action is required.

Severity

INFO

SEC-1126

Message

```
<timestamp>, [SEC-1126], <sequence-number>,, INFO, <system-name>,  
Secure mode has been disabled.
```

Probable Cause

Indicates that a secure mode disable operation completed successfully.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-1130

Message

```
<timestamp>, [SEC-1130], <sequence-number>,, INFO, <system-name>,  
The Primary FCS has failed over to a new switch.
```

Probable Cause

Indicates that an FCS failover operation was completed successfully.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-1135

Message

```
<timestamp>, [SEC-1135], <sequence-number>,, INFO, <system-name>,  
Secure fabric version stamp has been reset.
```

Probable Cause

Indicates that the version stamp of the secure fabric is reset.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-1136

Message

```
<timestamp>, [SEC-1136], <sequence-number>,, ERROR, <system-name>,  
Failed to verify signature <data type, MUA, policy, etc.,>.
```

Probable Cause

Indicates that the receiving switch fails to validate the security database sending from the primary FCS switch. This message usually indicates that the data package is corrupted, the time stamp on the package is out of range as a result of a replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure indicates either an internal error (such as losing the primary public key) or an invalid database.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that switch. This message might also be the result of an internal corruption or a hacker attack to the secure fabric.

Severity

ERROR

SEC-1137

Message

```
<timestamp>, [SEC-1137], <sequence-number>,, ERROR, <system-name>,  
No signature in <data type, MUA, policy, etc.,>.
```

Probable Cause

Indicates that the receiving switch fails to validate the security database sending from the primary FCS switch. This message usually indicates that the data package is corrupted, the time stamp on the package is out of range as a result of a replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure indicates either an internal error (such as losing the primary public key) or an invalid database.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that switch. This message might also be the result of an internal corruption or a hacker attack to the secure fabric.

Severity

ERROR

SEC-1138

Message

```
<timestamp>, [SEC-1138], <sequence-number>,, INFO, <system-name>,  
Security database download received from Primary FCS.
```

Probable Cause

Indicates that a non-primary FCS switch received a security database download.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-1139

Message

```
<timestamp>, [SEC-1139], <sequence-number>,, ERROR, <system-name>,  
The RSNMP_POLICY cannot exist without the WSNMP_POLICY.
```

Probable Cause

Indicates that the receiving switch fails to validate the security database sending from the primary FCS switch. This message usually indicates that the data package is corrupted, the time stamp on the package is out of range as a result of a replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure indicates either an internal error (such as losing the primary public key) or an invalid database.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that switch. This message might also be the result of an internal corruption or a hacker attack to the secure fabric.

Severity

ERROR

SEC-1142

Message

```
<timestamp>, [SEC-1142], <sequence-number>,, INFO, <system-name>,  
Reject new policies. <reason text>.
```

Probable Cause

Indicates that the new policies are rejected due to the reason specified.

Recommended Action

Use proper syntax when entering policy information.

Severity

INFO

SEC-1145

Message

```
<timestamp>, [SEC-1145], <sequence-number>,, INFO, <system-name>, A  
security admin event has occurred. This message is for information  
purpose only. The message for individual event is: <Event specific  
data>
```

Probable Cause

Indicates one of the following has occurred:

- The names for the specified policies have changed.
- The passwords have changed for the specified accounts.
- The SNMP community strings have been changed.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-1146

Message

```
<timestamp>, [SEC-1146], <sequence-number>,, INFO, <system-name>,  
PID changed: <State>.
```

Probable Cause

Indicates that the PID format of the switch was changed either to extended-edge PID or from extended-edge PID. If the DCC polices existed, all area ID values either increased or decreased by 16. The values wrap around after 128. If a DCC policy contains an area of 127 before changing to extended-edge PID, then the new area is 15, because of the wraparound.

Recommended Action

No action is required.

Severity

INFO

SEC-1153

Message

```
<timestamp>, [SEC-1153], <sequence-number>,, INFO, <system-name>,  
Error in RCA: RCS is not supported
```

Probable Cause

Indicates that RCS is not supported.

Recommended Action

Run the **rclInfoShow** command to view RCS capability on the fabric. RCS must be capable on all switches in the fabric to be enabled. If all switches are capable, it is automatically enabled.

For any switch that does not support RCS, obtain the latest firmware version from your switch supplier, and run the **firmwareDownload** command to upgrade the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

INFO

SEC-1154

Message

```
<timestamp>, [SEC-1154], <sequence-number>,, INFO, <system-name>,  
PID change failed: <Reason> <defined status> <active status>.
```

Probable Cause

Indicates that either the defined or the active policy could not be updated. If the policy database is very large, it might not be able to change the area because the new policy database exceeds the maximum size. This message can also be caused when the switch is short of memory. The status values can be either defined, active, or both. A negative value means that a policy set was failed by the daemon.

Recommended Action

Reduce the size of the policy database.

Severity

INFO

SEC-1155

Message

```
<timestamp>, [SEC-1155], <sequence-number>,, INFO, <system-name>,  
PID change failed: <Reason> <defined status> <active status>.
```

Probable Cause

Indicates that either the defined or active policy was too large after modifying the area ID. The status values can be either defined, active, or both. A negative value means that a policy set was failed by the daemon.

Recommended Action

Reduce the size of the specified policy database.

Severity

INFO

SEC-1156

Message

```
<timestamp>, [SEC-1156], <sequence-number>,, INFO, <system-name>,  
Change failed: <Reason> <defined status> <active status>.
```

Probable Cause

Indicates that the security daemon is busy. The status values can be either defined, active, or both. A negative value means that a policy set was failed by the daemon.

Recommended Action

For the first reject, wait a few minutes and then resubmit the transaction. Fabric-wide commands might take a few minutes to propagate throughout the fabric. Make sure to wait a few minutes between executing commands so that your commands do not overlap in the fabric.

Severity

INFO

SEC-1157

Message

```
<timestamp>, [SEC-1157], <sequence-number>,, INFO, <system-name>,  
PID Change failed: <Reason> <defined status> <active status>.
```

Probable Cause

Indicates that the provisioning resources for a security policy failed due to low memory or internal error. The status values can be either defined, active, or both. A negative value means that a policy set was failed by the daemon.

Recommended Action

Retry the failed command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

INFO

SEC-1158

Message

```
<timestamp>, [SEC-1158], <sequence-number>,, INFO, <system-name>,  
Invalid name <Policy or Switch name>.
```

Probable Cause

Indicates that the specified name is invalid. The name can be a policy name or a switch name.

Recommended Action

Enter a valid name.

Severity

INFO

SEC-1159

Message

```
<timestamp>, [SEC-1159], <sequence-number>,, INFO, <system-name>,  
Non_Reachable domain <Domain ID>.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

INFO

SEC-1160

Message

```
<timestamp>, [SEC-1160], <sequence-number>,, INFO, <system-name>,  
Duplicate port <Port ID> in port list (<Port list>).
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

INFO

SEC-1163

Message

```
<timestamp>, [SEC-1163], <sequence-number>,, ERROR, <system-name>,  
System is already in secure mode. Lockdown option cannot be applied.
```

Probable Cause

Indicates that the lockdown option was attempted while the fabric is already in secure mode.

Recommended Action

Do not use lockdown option with secModeEnable, when switch is already in secure mode.

Severity

ERROR

SEC-1164

Message

```
<timestamp>, [SEC-1164], <sequence-number>,, ERROR, <system-name>,  
Lockdown option cannot be applied on a non-FCS switch.
```

Probable Cause

Indicates that the attempt to enable security is made on a switch that is not present in the FCS list.

Recommended Action

Add the switch into the FCS policy list when using the lockdown option to enable security.

Severity

ERROR

SEC-1165

Message

```
<timestamp>, [SEC-1165], <sequence-number>,, ERROR, <system-name>,  
Low memory, failed to enable security on all switches.
```

Probable Cause

Indicates that the system is low on memory.

Recommended Action

Wait a few minutes and try the command again.

Severity

ERROR

SEC-1166

Message

```
<timestamp>, [SEC-1166], <sequence-number>,, ERROR, <system-name>,  
Non FCS tries to commit failover.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1167

Message

```
<timestamp>, [SEC-1167], <sequence-number>,, ERROR, <system-name>,  
Another FCS failover is in process. Command terminated.
```

Probable Cause

Indicates that because another failover is already in progress, this failover attempt cannot proceed.

Recommended Action

Verify that the security event was planned. If the security event was planned, retry FCS failover after current failover has completed, if this switch should become primary FCS. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

ERROR

SEC-1168

Message

```
<timestamp>, [SEC-1168], <sequence-number>,, ERROR, <system-name>,  
Primary FCS failover is busy. Please retry later.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1170

Message

```
<timestamp>, [SEC-1170], <sequence-number>,, INFO, <system-name>,  
This command must be executed on the Primary FCS switch, the first  
reachable switch in the FCS list.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

INFO

SEC-1171

Message

```
<timestamp>, [SEC-1171], <sequence-number>,, ERROR, <system-name>,  
Disabled secure mode due to invalid security object.
```

Probable Cause

Indicates that the switch is segmented, and secure mode is disabled on the switch because there was no license present or no PKI objects.

Recommended Action

Run the **pkiShow** command to check if all PKI objects exist. If they do not exist, run the **pkiCreate** command to create them for the switch.

Run the **licenseAdd** command to install the required license key. Refer to your switch supplier to obtain a license if you do not have one.

Severity

ERROR

SEC-1172

Message

```
<timestamp>, [SEC-1172], <sequence-number>,, ERROR, <system-name>,  
Failed to identify role.
```

Probable Cause

Indicates that the switch is unable to determine its role (primary FCS or backup FCS) in the secure fabric.

Recommended Action

Verify that all switches in the fabric are in time synchronization with the primary and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

Severity

ERROR

SEC-1173

Message

```
<timestamp>, [SEC-1173], <sequence-number>,, ERROR, <system-name>,  
Lost contact with Primary FCS switch.
```

Probable Cause

Indicates that the switch has lost contact with the primary FCS switch in the secure fabric. This could be due to the primary FCS being disabled.

Recommended Action

If the primary FCS was disabled intentionally, no action is required; if not, check the primary FCS.

Severity

ERROR

SEC-1174

Message

```
<timestamp>, [SEC-1174], <sequence-number>,, ERROR, <system-name>,  
Failed to set <FCS or non-FCS> password.
```

Probable Cause

Indicates that the FCS or non-FCS password could not be set.

Recommended Action

Verify that all switches in the fabric are in time synchronization with the primary and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

Severity

ERROR

SEC-1175

Message

```
<timestamp>, [SEC-1175], <sequence-number>,, ERROR, <system-name>,  
Failed to install zone data.
```

Probable Cause

Indicates that the zone database could not be installed on the switch.

Recommended Action

Verify that all switches in the fabric are in time synchronization with the primary and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

Severity

ERROR

SEC-1176

Message

```
<timestamp>, [SEC-1176], <sequence-number>,, ERROR, <system-name>,  
Failed to generate new version stamp.
```

Probable Cause

Indicates that the primary FCS failed to generate a new version stamp due to the fabric not being stable.

Recommended Action

Verify that all switches in the fabric are in time synchronization with the primary and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

Severity

ERROR

SEC-1180

Message

```
<timestamp>, [SEC-1180], <sequence-number>,, INFO, <system-name>,  
Added account <user name> with <role name> authorization.
```

Probable Cause

Indicates that the specified new account has been created.

Recommended Action

No action is required.

Severity

INFO

SEC-1181

Message

```
<timestamp>, [SEC-1181], <sequence-number>,, INFO, <system-name>,  
Deleted account <user name>
```

Probable Cause

Indicates that the specified account has been deleted.

Recommended Action

No action is required.

Severity

INFO

SEC-1182

Message

```
<timestamp>, [SEC-1182], <sequence-number>,, INFO, <system-name>,  
Recovered <number of> accounts.
```

Probable Cause

Indicates that the specified number of accounts have been recovered from backup.

Recommended Action

No action is required.

Severity

INFO

SEC-1183

Message

```
<timestamp>, [SEC-1183], <sequence-number>,, ERROR, <system-name>,  
Policy to binary conversion error: Port <port number> is out range.
```

Probable Cause

Indicates that a security database conversion has failed because of an invalid value.

Recommended Action

Retry the command with a valid value.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

SEC-1184

Message

```
<timestamp>, [SEC-1184], <sequence-number>,, INFO, <system-name>,  
Radius config change, action <action>, server ID <server>.
```

Probable Cause

Indicates that the specified action is applied to the specified RADIUS server configuration. The possible actions are ADD, REMOVE, CHANGE, and MOVE.

Recommended Action

No action is required.

Severity

INFO

SEC-1185

Message

```
<timestamp>, [SEC-1185], <sequence-number>,, INFO, <system-name>,  
<action> switch DB.
```

Probable Cause

Indicates that the switch database was enabled or disabled as the secondary AAA when RADUIS is the primary AAA mechanism.

Recommended Action

No action is required.

Severity

INFO

SEC-1186

Message

```
<timestamp>, [SEC-1186], <sequence-number>,, INFO, <system-name>,  
<action> Radius Configuration.
```

Probable Cause

Indicates that the RADIUS configuration was enabled or disabled as the primary AAA mechanism.

Recommended Action

No action is required.

Severity

INFO

SEC-1187

Message

```
<timestamp>, [SEC-1187], <sequence-number>,, INFO, <system-name>,  
Security violation: Unauthorized switch <switch wwn> tries to join  
secure fabric.
```

Probable Cause

Indicates that an SCC security violation was reported. The specified unauthorized switch attempts to join the secure fabric.

Recommended Action

Check the switch connection control policy (SCC policy specifies the WWNs of switches allowed in the fabric) to verify which switches are allowed in the fabric. If the switch should be allowed in the fabric but not included in the SCC policy, add the switch to the policy. If the switch is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity

INFO

SEC-1188

Message

```
<timestamp>, [SEC-1188], <sequence-number>,, INFO, <system-name>,  
Security violation: Unauthorized device <device node name> tries to  
flogin to area <port number> of switch <switch wwn>.
```

Probable Cause

Indicates that a DCC security violation was reported. The specified device attempted to login using FLOGI to an unauthorized port. The DCC policy correlates specific devices to specific port locations. If the device changes connected port, the device will not be allowed to login.

Recommended Action

Check DCC policy and verify that the specified device is allowed in the fabric and is included in the DCC policy. If the specified device not included in the policy, add it to the policy. If the host is not allowed

access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity

INFO

SEC-1189

Message

```
<timestamp>, [SEC-1189], <sequence-number>,, INFO, <system-name>,  
Security violation: Unauthorized host with IP address <IP address>  
tries to do SNMP write operation.
```

Probable Cause

Indicates that an SNMP security violation was reported. The specified unauthorized host attempted to perform a write SNMP operation.

Recommended Action

Check the WSNMP policy and verify which hosts are allowed access to the fabric through SNMP. If the host is allowed access to the fabric but is not included in the policy, add the host to the policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity

INFO

SEC-1190

Message

```
<timestamp>, [SEC-1190], <sequence-number>,, INFO, <system-name>,  
Security violation: Unauthorized host with IP address <IP address>  
tries to do SNMP read operation.
```

Probable Cause

Indicates that an SNMP security violation was reported. The specified unauthorized host attempted to perform a read SNMP operation.

Recommended Action

Check the RSNMP policy to verify that hosts allowed access to the fabric through SNMP read operations are included in the RSNMP policy. If the host is allowed access but is not included in the RSNMP policy, add the host to the policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity

INFO

SEC-1191

Message

```
<timestamp>, [SEC-1191], <sequence-number>,, INFO, <system-name>,  
Security violation: Unauthorized host with IP address <Ip address>  
tries to establish HTTP connection.
```

Probable Cause

Indicates that an HTTP security violation was reported. The specified unauthorized host attempted to establish an HTTP connection.

Recommended Action

Check if the host IP address specified in the message can be used to manage the fabric through an HTTP connection. If so, add the host IP address to the HTTP policy of the fabric. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity

INFO

SEC-1192

Message

```
<timestamp>, [SEC-1192], <sequence-number>,, INFO, <system-name>,  
Security violation: Login failure attempt via <connection method>.
```

Probable Cause

Indicates that a serial or modem login security violation was reported. The wrong password was used while trying to log in through a serial or modem connection; the login failed.

Recommended Action

Use the correct password.

Severity

INFO

SEC-1193

Message

```
<timestamp>, [SEC-1193], <sequence-number>,, INFO, <system-name>,  
Security violation: Login failure attempt via <connection method>.  
IP Addr: <IP address>
```

Probable Cause

Indicates that a specified login security violation was reported. The wrong password was used while trying to log in through the specified connection method; the login failed.

Recommended Action

The error message lists the violating IP address. Verify that this IP address is being used by a valid switch admin. Use the correct password.

Severity

INFO

SEC-1194

Message

```
<timestamp>, [SEC-1194], <sequence-number>,, WARNING,  
<system-name>, This switch does not have all the required PKI  
objects correctly installed.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

WARNING

SEC-1195

Message

```
<timestamp>, [SEC-1195], <sequence-number>,, WARNING,  
<system-name>, This switch has no <component> license.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

WARNING

SEC-1196

Message

```
<timestamp>, [SEC-1196], <sequence-number>,, WARNING,  
<system-name>, Switch does not have all default account names.
```

Probable Cause

Indicates that the default switch accounts admin and user do not exist on the switch when enabling security.

Recommended Action

Reset the default admin and user account names on the switch that reported the warning and retry enabling security.

Severity

WARNING

SEC-1197

Message

```
<timestamp>, [SEC-1197], <sequence-number>,, INFO, <system-name>,  
Changed account <user name>.
```

Probable Cause

Indicates that the specified account has changed.

Recommended Action

No action is required.

Severity

INFO

SEC-1198

Message

```
<timestamp>, [SEC-1198], <sequence-number>,, INFO, <system-name>,  
Security violation: Unauthorized host with IP address <IP address>  
tries to establish API connection.
```

Probable Cause

Indicates that an API security violation was reported. The specified unauthorized host attempted to establish an API connection.

Recommended Action

Check to see if the host IP address specified in the message can be used to manage the fabric through an API connection. If so, add the host IP address to the API policy of the fabric. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity

INFO

SEC-1199

Message

```
<timestamp>, [SEC-1199], <sequence-number>,, INFO, <system-name>,  
Security violation: Unauthorized access to serial port of switch  
<switch instance>.
```

Probable Cause

Indicates that a serial connection policy security violation was reported. An attempt was made to access the serial console on the specified switch instance when it is disabled.

Recommended Action

Check to see if an authorized access attempt is being made on the console. If so, add the switch WWN to the serial policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity

INFO

SEC-1200

Message

```
<timestamp>, [SEC-1200], <sequence-number>,, INFO, <system-name>,  
Security violation: MS command is forwarded from non-primary FCS  
switch.
```

Probable Cause

Indicates that an MS forward security violation was reported. A management server command was forwarded from a non-primary FCS switch.

Recommended Action

Check the MS policy and verify that the connection is allowed. If the connection is allowed but not specified, enable the connection in the MS policy. If the MS policy does not allow the connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity

INFO

SEC-1201

Message

```
<timestamp>, [SEC-1201], <sequence-number>,, INFO, <system-name>,  
Security violation: MS device <device wwn> operates on non-primary  
FCS switch.
```

Probable Cause

Indicates that an MS operation security violation was reported. An MS device operation occurred on a non-primary FCS switch.

Recommended Action

Check the management server policy and verify that the connection is allowed. If the connection is allowed but not specified, enable the connection in the MS policy. If the MS policy does not allow the connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity

INFO

SEC-1202

Message

```
<timestamp>, [SEC-1202], <sequence-number>,, INFO, <system-name>,  
Security violation: Unauthorized access from MS device node name  
<device node name>, device port name <device port name>.
```

Probable Cause

Indicates that a MS security violation was reported. The unauthorized device specified in the message attempted to establish a connection.

Recommended Action

Check the MS server policy and verify that the connection is allowed. If the connection is allowed but not specified, enable the connection in the MS policy. If the MS policy does not allow the connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity

INFO

SEC-1250

Message

```
<timestamp>, [SEC-1250], <sequence-number>,, WARNING,  
<system-name>, DCC enforcement API failed: <failed action>  
err=<status>, key=<data>
```

Probable Cause

Indicates that an internal error caused the DCC policy enforcement to fail.

Recommended Action

Retry the failed security command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

SEC-1251

Message

```
<timestamp>, [SEC-1251], <sequence-number>,, ERROR, <system-name>,  
Policy to binary conversion error: <text message> <value>.
```

Probable Cause

Indicates that the security database conversion failed because of invalid values. The reason is specified in the *text message* variable and faulty value is printed in *value* variable.

Recommended Action

Retry the failed security command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

SEC-1253

Message

```
<timestamp>, [SEC-1253], <sequence-number>,, ERROR, <system-name>,  
Bad DCC interface state during <Phase>, state=<state>.
```

Probable Cause

Indicates that an internal error has caused the DCC policy update to fail in the provision, commit, or cancel phases.

Recommended Action

Retry the failed security command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

SEC-1300

Message

```
<timestamp>, [SEC-1300], <sequence-number>,, INFO, <system-name>,  
This switch is in VcEncode mode. Security is not supported.
```

Probable Cause

Indicates that the switch is set up with VC-encoded mode.

Recommended Action

Turn off VC-encoded mode before enabling security.

Severity

INFO

SEC-1301

Message

```
<timestamp>, [SEC-1301], <sequence-number>,, INFO, <system-name>,  
This switch is in interop mode. Security is not supported.
```

Probable Cause

Indicates that the switch is interop-mode enabled.

Recommended Action

Disable interop-mode using the interopMode command before enabling the Secure Fabric OS feature.

Severity

INFO

SEC-1302

Message

```
<timestamp>, [SEC-1302], <sequence-number>,, INFO, <system-name>,  
This switch does not have all the required PKI objects correctly  
installed.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

INFO

SEC-1303

Message

```
<timestamp>, [SEC-1303], <sequence-number>,, INFO, <system-name>,  
This software version does not support security.
```

Probable Cause

Indicates that the currently installed software version does not support the HP StorageWorks Secure Fabric OS feature.

Recommended Action

Run the **firmwareDownload** command to update the firmware to the latest version for your specific switch. Verify that the firmware you are installing supports the HP StorageWorks Secure Fabric OS feature.

Severity

INFO

SEC-1304

Message

```
<timestamp>, [SEC-1304], <sequence-number>,, INFO, <system-name>,  
This switch has no security license.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

INFO

SEC-1305

Message

```
<timestamp>, [SEC-1305], <sequence-number>,, INFO, <system-name>,  
This switch has no zoning license.
```

Probable Cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

INFO

SEC-1306

Message

```
<timestamp>, [SEC-1306], <sequence-number>,, INFO, <system-name>,  
Failed to verify certificate with root CA.
```

Probable Cause

Indicates that the certificate could not be verified with root certificate authority (CA). This could happen if an unauthorized switch tries to access the fabric that is not certified by a trusted root CA or a root CA certificate does not exist on the switch.

Recommended Action

Run the **pkiShow** command and verify that all PKI objects exist on the switch. If a failure to validate PKI objects occurs, follow the steps for re-creating PKI objects outlined in the *Secure Fabric OS User's Guide*. If PKI objects are valid, verify that an unauthorized switch is not trying to access the fabric.

Severity

INFO

SEC-1307

Message

```
<timestamp>, [SEC-1307], <sequence-number>,, INFO, <system-name>,  
Got response from Radius server <Radius server identity>.
```

Probable Cause

Indicates that after some servers timed out, the specified RADIUS server responded to a switch request.

Recommended Action

If the message appears frequently, move the responding server to the top of the RADIUS server configuration list using the **aaaConfig** command.

Severity

INFO

SEC-1308

Message

```
<timestamp>, [SEC-1308], <sequence-number>,, INFO, <system-name>,  
All Radius servers have failed to respond.
```

Probable Cause

Indicates that all servers in the RADIUS configuration have failed to respond to a switch request within the specified timeout.

Recommended Action

Verify that the switch has proper network connectivity to the specified RADIUS servers, and the servers are correctly configured.

Severity

INFO

SEC-1309

Message

```
<timestamp>, [SEC-1309], <sequence-number>,, INFO, <system-name>,  
Waiting for RCS transaction to complete: <Wait time in seconds> secs
```

Probable Cause

Indicates that Secure Fabric OS is still waiting for the RCS transaction to complete.

Recommended Action

Verify if there are any RCS or RTWR errors. If not, the transaction is still in progress.

Severity

INFO

SEC-3001

Message

```
<timestamp>, [SEC-3001], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: security mode <State change:  
Enabled or Disabled>.
```

Probable Cause

Indicates that the security mode of the fabric was either enabled or disabled.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3002

Message

```
<timestamp>, [SEC-3002], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: NONE
```

Probable Cause

Indicates that the specified security event has occurred. The event can be:

- There has been an FCS failover.
- A security policy has been activated.
- A security policy has been saved.
- A security policy has been aborted.
- A non-FCS password has changed.
- A temporary password was set or reset.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3003

Message

```
<timestamp>, [SEC-3003], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: Create <Policy Name> policy,  
with <Member List> entries.
```

Probable Cause

Indicates that a new security policy with entries has been created. When you use a wildcard (for example, an asterisk) in creating a policy, the audit report displays the wildcard in the event info field.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3004

Message

```
<timestamp>, [SEC-3004], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: Create <Policy name> policy.
```

Probable Cause

Indicates that a new security policy has been created. When you use a wildcard (for example, an asterisk) in creating member for a policy, the audit report displays the wildcard in the event info field.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3005

Message

```
<timestamp>, [SEC-3005], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: Add members [<Members added>]  
to policy <Policy name>.
```

Probable Cause

Indicates that new member(s) have been added to a security policy. When you use a wildcard (for example, an asterisk) in adding members to a policy, the audit report displays the wildcard in the event info field.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3006

Message

```
<timestamp>, [SEC-3006], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: Remove members [<Members  
removed>] from policy <Policy name>.
```

Probable Cause

Indicates that a user has removed the specific members from the security policy. When you use a wildcard (for example, an asterisk) in removing members from a policy, the audit report displays the wildcard in the event info field.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3007

Message

```
<timestamp>, [SEC-3007], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: Delete policy <Deleted policy  
name>.
```

Probable Cause

Indicates that the user deleted the specified security policy.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3008

Message

```
<timestamp>, [SEC-3008], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: FCS moved from position [<Old  
FCS position>] to [<New FCS position>].
```

Probable Cause

Indicates that the FCS list has been modified. One of the members of the list has been moved to a new position in the list.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3009

Message

```
<timestamp>, [SEC-3009], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: Security Transaction aborted.
```

Probable Cause

Indicates that the pending security transaction is aborted.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3010

Message

```
<timestamp>, [SEC-3010], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: Reset [<Event specific  
information>] security stat(s).
```

Probable Cause

Indicates that the user has reset all the security statistics.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3011

Message

```
<timestamp>, [SEC-3011], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: Reset <Stat name> stat on  
domains <Domain IDs>.
```

Probable Cause

Indicates that the user has reset a security statistic on the specified domains.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3012

Message

```
<timestamp>, [SEC-3012], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: Passwd set/reset on domain  
[<Domain ID>] for account(s) <Account name>.
```

Probable Cause

Indicates that the user has reset the password for the specified user accounts.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3013

Message

```
<timestamp>, [SEC-3013], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: Version is reset.
```

Probable Cause

Indicates that the specified user has reset the security version stamp.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3014

Message

```
<timestamp>, [SEC-3014], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: <Event option> server <Event  
data>.
```

Probable Cause

Indicates that the specified user has changed the RADIUS configuration.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3015

Message

```
<timestamp>, [SEC-3015], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: <Event option> server <Server  
name> to position <New position>.
```

Probable Cause

Indicates that the specified user has changed the position of the RADIUS server.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-

Message

```
<timestamp>, [SEC-], <sequence-number>, AUDIT, INFO, <system-name>,  
User: <User Name>, Role: <User Role>, Event: <Event Name>, Status:  
<Event Status>, Info: <Event option> server <server ID> attributes.  
New values: <Changed values>
```

Probable Cause

Indicates that the specified user has changed the attributes of the RADIUS server.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3017

Message

```
<timestamp>, [SEC-3017], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: Radius <Server state>
```

Probable Cause

Indicates that the specified user has changed the RADIUS configuration.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SNMP Error Messages

SNMP-1001

Message

```
<timestamp>, [SNMP-1001], <sequence-number>,, ERROR, <system-name>,  
SNMP service is not available <Reason>.
```

Probable Cause

Indicates that the SNMP service could not be started because of the specified *Reason*. You will not be able to query the switch through SNMP.

Recommended Action

Verify that the IP address for the Ethernet and Fibre Channel interface is set correctly. If the specified *Reason* is an initialization failure, the switch requires a reboot.

Severity

ERROR

SNMP-1002

Message

```
<timestamp>, [SNMP-1002], <sequence-number>,, ERROR, <system-name>,  
SNMP <Error Details> initialization failed.
```

Probable Cause

Indicates that the initialization of the SNMP service failed and you will not be able to query the switch through SNMP.

Recommended Action

Reboot or power cycle the switch. This will automatically initialize SNMP.

Severity

ERROR

SNMP-1003

Message

```
<timestamp>, [SNMP-1003], <sequence-number>,, ERROR, <system-name>,  
Distribution of Community Strings to Secure Fabric failed.
```

Probable Cause

Indicates that the changes in the SNMP community strings could not be propagated to other switches in the secure fabric.

Recommended Action

Retry changing the SNMP community strings from the primary switch.

Severity

ERROR

SNMP-1004

Message

```
<timestamp>, [SNMP-1004], <sequence-number>,, ERROR, <system-name>,  
Incorrect SNMP configuration.
```

Probable Cause

Indicates that the SNMP configuration is incorrect and the SNMP service will not work correctly.

Recommended Action

Change the SNMP configuration back to the default.

Severity

ERROR

SS Error Messages

SS-1000

Message

```
<timestamp>, [SS-1000], <sequence-number>,, INFO, <system-name>,  
supportSave has ftp'ed support information to the host with IP  
address <host ip>.
```

Probable Cause

Indicates that the **supportSave** command was used to transfer support information to a remote FTP location.

Recommended Action

No action is required.

Severity

INFO

SS-1001

Message

```
<timestamp>, [SS-1001], <sequence-number>,, WARNING, <system-name>,  
supportSave's ftp operation to host IP address <host ip> aborted.
```

Probable Cause

Indicates that an FTP error occurred during execution of the **supportSave** command.

Recommended Action

Check the FTP server and settings. Run the **supportFtp** command to set the FTP parameters. After the FTP problem is corrected, rerun the **supportSave** command.

Severity

WARNING

LB Error Messages

SULB-1001

Message

```
<timestamp>, [SULB-1001], <sequence-number>,, WARNING,  
<system-name>, Firmwaredownload command has started.
```

Probable Cause

Indicates that the **firmwareDownload** command has started. This process can take some time; wait until the process is complete before initiating any new commands to the system.

Recommended Action

Do not fail over or power down the system during firmware upgrade. Allow the **firmwareDownload** command to continue without disruption. No action is required.

Run the **firmwareDownloadStatus** command for more information.

Severity

WARNING

SULB-1002

Message

```
<timestamp>, [SULB-1002], <sequence-number>,, INFO, <system-name>,  
Firmwaredownload command has completed successfully.
```

Probable Cause

Indicates that the **firmwareDownload** command has completed successfully and loaded firmware to both the CPs.

Recommended Action

No action is required. The **firmwareDownload** command has completed as expected.

Run the **firmwareDownloadStatus** command for more information.

Severity

INFO

SULB-1003

Message

```
<timestamp>, [SULB-1003], <sequence-number>,, INFO, <system-name>,  
Firmwarecommit has started.
```

Probable Cause

Indicates the **firmwareCommit** or **firmwareRestore** command has started to update the secondary partition.

Recommended Action

No action is required. Run the **firmwareDownloadStatus** command for more information.

Severity

INFO

SULB-1005

Message

```
<timestamp>, [SULB-1005], <sequence-number>,, INFO, <system-name>,  
Current Active CP is preparing to failover.
```

Probable Cause

Indicates that the forced failover was successful and the standby CP is now the active CP.

Recommended Action

No action is required. The **firmwareDownload** command is progressing as expected.

Run the **firmwareDownloadStatus** command for more information.

Severity

INFO

SULB-1006

Message

```
<timestamp>, [SULB-1006], <sequence-number>,, INFO, <system-name>,  
Forced failover succeeded. New Active CP is running new firmware.
```

Probable Cause

Indicates that the previous standby has now become the active CP and is running the new firmware version.

Recommended Action

No action is required. The **firmwareDownload** command is progressing as expected.

Run the **firmwareDownloadStatus** command for more information.

Severity

INFO

SULB-1007

Message

```
<timestamp>, [SULB-1007], <sequence-number>,, INFO, <system-name>,  
Standby CP reboots.
```

Probable Cause

Indicates that the standby CP will reboot.

Recommended Action

No action is required. The **firmwareDownload** command is progressing as expected.

Run the **firmwareDownloadStatus** command for more information.

Severity

INFO

SULB-1008

Message

```
<timestamp>, [SULB-1008], <sequence-number>,, INFO, <system-name>,  
Standby CP booted successfully with new firmware.
```

Probable Cause

Indicates that the standby CP has rebooted successfully.

Recommended Action

No action is required. The **firmwareDownload** command is progressing as expected.

Run the **firmwareDownloadStatus** command for more information.

Severity

INFO

SULB-1009

Message

```
<timestamp>, [SULB-1009], <sequence-number>,, INFO, <system-name>,  
Firmwaredownload command failed (0x<firmwaredownload error code>).
```

Probable Cause

Indicates that the firmware download failed. The additional *error message* information provides debugging information.

The **firmwareDownload** error code contains two bytes. The first byte contains the upgrade error message code, as indicated in the first table below, while the second byte might contain either the reason code (what caused the failure) or the state code (where the failure occurs), as indicated in the second table below. The error code can be retrieved either by running the **firmwareDownloadStatus** command or through the **errShow** and **errDump** commands.

For example, the following entry indicates that the **firmwareDownload** failed in SUS_SBY_FS_CHECK (0x2e) state because the "Standby CP failed to reboot" (0x66):

Switch: 0, Info SULIB-FWDL_FAIL, 4, Firmwaredownload command failed (status=0x662e)

The following entry indicates that the **firmwareDownload** failed (0x44) because firmware has not been committed (0x1e):

Switch: 0, Info SULIB-FWDL_FAIL, 4, Firmwaredownload command failed (status=0x441e)

Table 5 lists the upgrade message and the associated code for that message.

Table 5 Upgrade messages and code values

Upgrade messages	Code
"Image is up-to-date. No need to download."	0xF
"Boot environment variable is inconsistent."	0x10
"Bootenv OSRootPartition is inconsistent."	0x11
"Can't access package list (.plist) file."	0x12
"RPM database is inconsistent."	0x13
"Ran out of memory."	0x14
"Firmwaredownload failed due to out of disk space or timeout."	0x15
"Failed to create firmware version file."	0x16
"Unexpected system error."	0x17
"Error in getting lock device."	0x18
"Error in releasing lock device."	0x19
"Firmwarecommit failed."	0x1a
"Firmware directory structure is not compatible."	0x1b
"Failed to load kernel image."	0x1c
"Bootenv OSLoader is inconsistent."	0x1d
"Firmwaredownload failed because new image has not been committed."	0x1e
"Firmwarerestore failed."	0x1f
"Both images are mounted to the same device."	0x20
"Error in removing packages."	0x21
"Firmwaredownload is already in progress."	0x22
"Firmwaredownload timeout."	0x23
"Firmwaredownload sanity check failed."	0x30
"Sanity check failed because system is non-redundant."	0x31
"Sanity check failed because firmwareDownload is already in progress."	0x32
"Sanity check failed because FABRIC OS is disabled on Active CP."	0x33
"Sanity check failed because HAMD is disabled on Active CP."	0x34
"Sanity check failed because firmwareDownload is already in progress."	0x35
"Sanity check failed because FABRIC OS is disabled on Standby CP."	0x36
"Sanity check failed because HAMD is disabled on Standby CP."	0x37
"Firmwaredownload failed on Standby CP."	0x40
"Firmwaredownload failed on Standby CP."	0x41
"Firmwaredownload failed on Standby CP."	0x42
"Firmwarecommit failed on Standby CP."	0x43
"Firmwaredownload failed."	0x44

Table 5 Upgrade messages and code values (continued)

Upgrade messages	Code
"Firmwaredownload failed due to Standby CP timeout."	0x50
"Unable to check firmware version due to Standby CP timeout."	0x51
"Firmwaredownload failed due to Standby CP timeout."	0x52
"Firmwaredownload failed due to Standby CP timeout."	0x53
"Standby CP failed to reboot and was not responding."	0x54
"Firmwarecommit failed due to Standby CP timeout."	0x55
"Unable to check firmware version due to Standby CP timeout."	0x56
"Unable to restore the original firmware due to Standby CP timeout."	0x57
"Standby CP failed to reboot and was not responding."	0x58
"Unable to check firmware version due to Standby CP timeout."	0x59
"Sanity check failed because firmwareDownload is already in progress."	0x60
"Sanity check failed because firmwareDownload is already in progress."	0x61
NOT USED	0x62
"System Error."	0x63
"Active CP forced failover succeeded. Now this CP becomes Active."	0x64
"Standby CP booted up."	0x65
"Standby CP failed to reboot."	0x66
"Standby rebooted successfully."	0x67
"Standby failed to reboot."	0x68
"Firmwarecommit has started to restore the secondary partition."	0x69
"Local CP is restoring its secondary partition."	0x6a
"Unable to restore the secondary partition. Please use firmwaredownloadstatus and firmwareshow to see firmware status."	0x6b
"Firmwaredownload has started on Standby CP. It might take up to 10 minutes."	0x6c
"Firmwaredownload has completed successfully on Standby CP."	0x6d
"Standby CP reboots."	0x6e
"Standby CP failed to boot up."	0x6f
"Standby CP booted up with new firmware."	0x70
"Standby CP failed to boot up with new firmware."	0x71
"Firmwaredownload has completed successfully on Standby CP."	0x72
"Firmwaredownload has started on Standby CP. It might take up to 10 minutes. "	0x73
"Firmwaredownload has completed successfully on Standby CP."	0x74
"Standby CP reboots."	0x75
"Standby CP failed to reboot."	0x76

Table 5 Upgrade messages and code values (continued)

Upgrade messages	Code
"Firmwarecommit has started on Standby CP."	0x77
"Firmwarecommit has completed successfully on Standby CP."	0x78
"Standby CP booted up with new firmware."	0x79
"Standby CP failed to boot up with new firmware."	0x7a
"Firmwarecommit has started on both Active and Standby CPs."	0x7b
"Firmwarecommit has completed successfully on Active CP."	0x7c
"Firmwarecommit failed on Active CP."	0x7d
"The original firmware has been restored successfully on Standby CP."	0x7e
"Unable to restore the original firmware on Standby CP."	0x7f
"Standby CP reboots."	0x80
"Standby CP failed to reboot."	0x81
"Standby CP booted up with new firmware."	0x82
"Standby CP failed to boot up with new firmware."	0x83
"There was an unexpected reboot during firmwareDownload . The command is aborted."	0x84
"Standby CP was not responding. The command is aborted."	0x85
"Firmwarecommit has started on both CPs. Please use firmwaredownloadstatus and firmwareshow to see the firmware status."	0x86
"Firmwarecommit has started on the local CP. Please use firmwaredownloadstatus and firmwareshow to see the firmware status."	0x87
"Firmwarecommit has started on the remote CP. Please use firmwaredownloadstatus and firmwareshow to see the firmware status."	0x88
"Please use firmwaredownloadstatus and firmwareshow to see the firmware status."	0x89
"Firmwaredownload command has completed successfully."	0x8a
"The original firmware has been restored successfully."	0x8b
"Remote CP is restoring its secondary partition."	0x8c
"Local CP is restoring its secondary partition."	0x8d
"Remote CP is restoring its secondary partition."	0x8e
"Firmwaredownload has started."	0x8f
"Firmwarecommit has started."	0x90
"Firmwaredownload has completed successfully."	0x91
"Firmwarecommit has completed successfully."	0x92
"Firmwarecommit has started to restore the secondary partition."	0x93
"Firmwarecommit failed."	0x94
"The secondary partition has been restored successfully."	0x95

Table 6 lists the upgrade state and the associated code value for that state. This information is transient within the Boot ROM environment and is provided here only for assisting support personnel in the debug process.

Table 6 Upgrade state and code value

Upgrade State	Code
SUS_PEER_CHECK_SANITY	0x21
SUS_PEER_FWDL_BEGIN	0x22
SUS_SBY_FWDL_BEGIN	0x23
SUS_PEER_REBOOT	0x24
SUS_SBY_REBOOT	0x25
SUS_SBY_FABOS_OK	0x26
SUS_PEER_FS_CHECK	0x27
SUS_SELF_FAILOVER	0x28
SUS_SBY_FWDL1_BEGIN	0x29
SUS_SELF_FWDL_BEGIN	0x2a
SUS_SELF_COMMIT	0x2b
SUS_SBY_FWC_BEGIN	0x2c
SUS_SBY_COMMIT	0x2d
SUS_SBY_FS_CHECK	0x2e
SUS_ACT_FWC_BEGIN	0x2f
SUS_PEER_RESTORE_BEGIN	0x30
SUS_SBY_RESTORE_BEGIN	0x31
SUS_PEER_FWC_BEGIN	0x32
SUS_PEER_FS_CHECK1	0x33
SUS_FINISH	0x34
SUS_COMMIT	0x35

Recommended Action

Run the **firmwareDownload** status command for more information.

Refer to the *HP StorageWorks Fabric OS 5.x administrator guide* for troubleshooting information.

Severity

INFO

SULB-1010

Message

```
<timestamp>, [SULB-1010], <sequence-number>,, INFO, <system-name>,
Firmwarecommit failed (status=0x<firmwarecommit error code>).
```

Probable Cause

Indicates that a firmware commit failed to update the secondary partition.

Recommended Action

Run the **firmwareCommit** command.

If this message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

INFO

SWCH Error Messages

SWCH-1001

Message

```
<timestamp>, [SWCH-1001], <sequence-number>,, ERROR, <system-name>,  
Switch is not in ready state - Switch enable failed switch status=  
0x<switch status>, c_flags = 0x<switch control flags>
```

Probable Cause

Indicates that the switch is enabled before it is ready.

Recommended Action

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

SWCH-1002

Message

```
<timestamp>, [SWCH-1002], <sequence-number>,, INFO, <system-name>,  
Security violation: Unauthorized device <wwn name of device> tries  
to flogin to port <port number>
```

Probable Cause

Indicates that the device is not present in the authorized profile list.

Recommended Action

Verify that the device is authorized to log in to the switch. If the device is authorized, run the **secPolicyDump** command to verify whether the specified device WWN is listed. If it is not listed, run the **secPolicyAdd** command to add this device to an existing policy.

Severity

INFO

SWCH-1003

Message

```
<timestamp>, [SWCH-1003], <sequence-number>,, ERROR, <system-name>,  
Slot ENABLED but Not Ready during recovery, disabling slot = <slot  
number>(<return value>)
```

Probable Cause

Indicates that the slot state has been detected as inconsistent during failover or recovery.

Recommended Action

On a Core Switch 2/64, SAN Director 2/128, or 4/256 SAN Director switch, run the **slotPowerOff** and then the **slotPowerOn** command.

On a 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, or SAN Switch 4/32 switch, reboot or power cycle the switch.

Severity

ERROR

SWCH-1004

Message

```
<timestamp>, [SWCH-1004], <sequence-number>,, ERROR, <system-name>,  
Blade attach failed during recovery, disabling slot = <slot number>
```

Probable Cause

Indicates that a blade has failed during failover or recovery.

Recommended Action

On a Core Switch 2/64, SAN Director 2/128, or 4/256 SAN Director switch, run the **slotPowerOff** and then the **slotPowerOn** command.

On a 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, or SAN Switch 4/32 switch, reboot or power cycle the switch.

Severity

ERROR

SWCH-1005

Message

```
<timestamp>, [SWCH-1005], <sequence-number>,, ERROR, <system-name>,  
Diag attach failed during recovery, disabling slot = <slot number>
```

Probable Cause

Indicates that the Diag blade attach has failed during failover or recovery.

Recommended Action

On a Core Switch 2/64, SAN Director 2/128, or 4/256 SAN Director switch, run the **slotPowerOff** and then the **slotPowerOn** command.

On a 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, or SAN Switch 4/32 switch, reboot or power cycle the switch.

Severity

ERROR

SYSC Error Messages

SYSC-1001

Message

```
<timestamp>, [SYSC-1001], <sequence-number>,, CRITICAL,  
<system-name>, Failed to run <Name of program that could not be run  
(string)>:<System internal error message (string)>
```

Probable Cause

Indicates that during the boot sequence, one of the programs would not run on the system.

Recommended Action

If the message is reported during a reboot after new firmware has been loaded, try reloading the firmware using the **firmwareDownload** command.

If the message persists, there might be a conflict between the two versions of firmware or the nonvolatile storage might be corrupted.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

CRITICAL

SYSC-1002

Message

```
<timestamp>, [SYSC-1002], <sequence-number>,, CRITICAL,  
<system-name>, Switch bring-up timed out
```

Probable Cause

Indicates that the system timed out during a reboot or failover sequence, waiting for one or more programs to register with system services or to fail over to active status.

Recommended Action

The switch is in an inconsistent state and can be corrected only by a reboot or power cycle. Before rebooting the chassis, record the firmware version on the switch (or CP) and run the **haDump** command. If this is a dual-CP switch, then gather the output from the CP in which this log message appeared.

Severity

CRITICAL

SYSC-1003

Message

```
<timestamp>, [SYSC-1003], <sequence-number>,, CRITICAL,  
<system-name>, Chassis config option <Option number read from the  
chassis option storage device> is not supported by CP blade with ID  
<Blade ID (platform) number from Active CP>. Change the chassis  
configuration.
```

Probable Cause

Indicates that during system startup the option configuration file corresponding to the chassis config option read could not be found. This indicates that the option is not supported on this platform running this version of the command.

It could also indicate that the current option number could not be read from the chassis option storage device (the WWN card).

This message only occurs on the SAN Director 2/128 and 4/256 SAN Director.

Recommended Action

Use the **chassisConfig** command to change chassis config mode to a setting that is valid for this platform running this firmware level. Chassis config mode 1 is valid for all platforms running all levels of firmware.

Severity

CRITICAL

SYSM Error Messages

SYSM-1001

Message

```
<timestamp>, [SYSM-1001], <sequence-number>,, CRITICAL,  
<system-name>, No memory
```

Probable Cause

Indicates that the switch has run out of system memory.

Recommended Action

Run the **memShow** command to view the switch memory usage.

Reboot or power cycle the switch.

Run **supportFtp** and **traceFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

CRITICAL

SYSM-1002

Message

```
<timestamp>, [SYSM-1002], <sequence-number>,, INFO, <system-name>,  
<number>, Switch: <Switch number>
```

Probable Cause

Indicates that a user has executed either the **switchShutdown** or **switchReboot** command. All services are brought down for a logical switch.

Recommended Action

No action is required if the **switchShutdown** or **switchReboot** command was executed intentionally. If the **switchShutdown** command was run, you must run the **switchStart** command to restart traffic on the logical switch.

Severity

INFO

SYSM-1003

Message

```
<timestamp>, [SYSM-1003], <sequence-number>,, INFO, <system-name>,  
<number>, Switch: <start reason>
```

Probable Cause

Indicates that the user executed the **switchStart** or **switchReboot** command. This indicates that all services are brought back up after a temporary shutdown of that logical switch.

Recommended Action

No action is required if the **switchStart** command was executed intentionally. Because reinitializing a switch is a disruptive operation and can stop I/O traffic, you might have to stop and restart the traffic during this process.

Severity

INFO

SYSM-1004

Message

```
<timestamp>, [SYSM-1004], <sequence-number>,, ERROR, <system-name>,  
Failed to retrieve current chassis configuration option,  
ret=<Unknown>
```

Probable Cause

Indicates that there was a failure to read configuration data from the WWN card.

Recommended Action

Verify that the WWN card is present and operational and that the affected CP is properly seated in its slot.

Severity

ERROR

TRCE Error Messages

TRCE-1001

Message

```
<timestamp>, [TRCE-1001], <sequence-number>,, WARNING,  
<system-name>, Trace dump available< optional slot indicating on  
which slot the dump occurs >! (reason: <Text explanation of what  
triggered the dump. (PANIC DUMP, WATCHDOG EXPIRED, MANUAL,  
TRIGGER)>)
```

Probable Cause

Indicates that trace dump files have been generated on the switch or the indicated slot. The reason field indicates the cause for generating the dump:

- PANICDUMP generated by panic dump
- WATCHDOG EXPIRED generated by hardware watchdog expiration
- MANUAL generated by the **traceDump -n** command
- TRIGGER when triggered by a specific Message ID generated by CRITICAL RASLog message or RASLog message trigger setup using the **traceTrig** command

Recommended Action

Run **supportFtp** and **traceFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

TRCE-1002

Message

```
<timestamp>, [TRCE-1002], <sequence-number>,, INFO, <system-name>,
Trace dump< optional slot indicating on which slot the dump occurs >
automatically transferred to FTP address ' <FTP target designated
by user> '.
```

Probable Cause

Indicates that a trace dump has occurred on the switch or the indicated slot and is successfully transferred from the switch automatically.

Recommended Action

No action is required.

Severity

INFO

TRCE-1003

Message

```
<timestamp>, [TRCE-1003], <sequence-number>,, ERROR, <system-name>,
Trace dump< optional slot indicating on which slot the dump occurs >
was not transferred due to FTP error.
```

Probable Cause

Indicates that a trace dump has been created on the switch or the indicated slot but is not automatically transferred from the switch due to an FTP error, such as wrong FTP address, FTP site down, or the network is down.

Recommended Action

Verify that the FTP parameters specified in **supportFtp** are correct.

Verify that the FTP parameters specified in **traceFtp** are correct.

Verify that the switch is connected to your Ethernet network.

Verify that the your network is up and running.

Severity

ERROR

TRCE-1004

Message

```
<timestamp>, [TRCE-1004], <sequence-number>,, WARNING,  
<system-name>, Trace dump< optional slot indicating on which slot  
the dump occurs > was not transferred because trace auto-FTP  
disabled.
```

Probable Cause

Indicates that trace dump files have been created on the switch or the indicated slot but are not automatically transferred from the switch because auto-FTP is disabled.

Recommended Action

Run **supportFtp** to set up and enable automatic FTP transfers.

Run **traceFtp** to set up and enable automatic FTP transfers.

Severity

WARNING

TRCE-1005

Message

```
<timestamp>, [TRCE-1005], <sequence-number>,, ERROR, <system-name>,  
FTP Connectivity Test failed due to error.
```

Probable Cause

Indicates that the connectivity test to the FTP host failed. This is usually caused by problems such as a wrong FTP address, FTP server being down, or the network being down.

Recommended Action

Verify that the FTP parameters specified in **supportFtp** are correct.

Verify that the FTP parameters specified in **traceFtp** are correct.

Verify that the switch is connected to your Ethernet network.

Verify that the your network is up and running.

Severity

ERROR

TRCE-1006

Message

```
<timestamp>, [TRCE-1006], <sequence-number>,, INFO, <system-name>,  
FTP Connectivity Test succeeded to FTP site ' <FTP target configured  
by users.> '.
```

Probable Cause

Indicates that a connectivity test to the FTP host has succeeded.

Recommended Action

No action is required.

Severity

INFO

TRCE-1007

Message

```
<timestamp>, [TRCE-1007], <sequence-number>,, ERROR, <system-name>,  
Notification of this CP has failed. Parameters temporarily out of  
synch with other CP.
```

Probable Cause

Indicates that the active CP is unable to alert the standby CP of a change in trace status. This message is only applicable to the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.

Recommended Action

This message is often transitory. Wait a few minutes and try the command again.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

TRCE-1008

Message

```
<timestamp>, [TRCE-1008], <sequence-number>,, CRITICAL,  
<system-name>, Unable to load trace parameters.
```

Probable Cause

Indicates that the active CP is unable to read stored trace parameters.

Recommended Action

Run the **haFailover** command to switch to the standby CP. Once the fail over is complete, then reboot the new standby CP.

Run **traceFtp** to set up and enable automatic FTP transfers of trace files.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

CRITICAL

TRCE-1009

Message

```
<timestamp>, [TRCE-1009], <sequence-number>,, ERROR, <system-name>,  
Unable to alert active CP that a dump has occurred.
```

Probable Cause

Indicates that the standby CP is unable to communicate trace information to active CP. This message is only applicable to the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.

Recommended Action

Run the **haShow** command to verify that the current CP is standby and the active CP is active.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command on both CPs and contact your switch service provider.

Severity

ERROR

TRCE-1010

Message

```
<timestamp>, [TRCE-1010], <sequence-number>,, ERROR, <system-name>,  
Traced fails to start
```

Probable Cause

Indicates that the trace daemon (traced), used for transferring trace files, failed to start. The trace capability within the switch is unaffected.

Recommended Action

Run **traceFtp** to set up for automatic FTP transfers.

Reboot the CP (dual-CP system) or restart the switch.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

TRCE-1011

Message

```
<timestamp>, [TRCE-1011], <sequence-number>,, INFO, <system-name>,  
Trace dump manually transferred to target ' <optional string to  
indicate which slot the dump is ftped out.> ': <result>.
```

Probable Cause

Indicates that a manual transfer of trace dump files has occurred.

Recommended Action

No action is required.

Severity

INFO

TRCK Error Messages

TRCK-1001

Message

```
<timestamp>, [TRCK-1001], <sequence-number>,, INFO, <system-name>,  
Successful login by user <User>.
```

Probable Cause

Indicates that the track change feature recorded a successful login.

Recommended Action

No action is required.

Severity

INFO

TRCK-1002

Message

```
<timestamp>, [TRCK-1002], <sequence-number>,, INFO, <system-name>,  
Unsuccessful login by user <User>.
```

Probable Cause

Indicates that the track change feature recorded a failed login. This occurs if the user name or password is entered incorrectly.

Recommended Action

Normally, this message indicates a typing error by an authorized user. If this message occurs repeatedly, it might indicate an unauthorized user trying to gain access to a switch. When secure mode is enabled on the fabric, the IP address of a failed login is reported to the error log.

Severity

INFO

TRCK-1003

Message

```
<timestamp>, [TRCK-1003], <sequence-number>,, INFO, <system-name>,  
Logout by user <User>.
```

Probable Cause

Indicates that the track change feature recorded a successful logout.

Recommended Action

No action is required.

Severity

INFO

TRCK-1004

Message

```
<timestamp>, [TRCK-1004], <sequence-number>,, INFO, <system-name>,  
Config file change from task:<task>
```

Probable Cause

Indicates that the track change feature recorded a configuration change for the switch. The track change feature records any change to the configuration file in nonvolatile memory, including a **configDownload**. This message is not generated for a **configUpload**. All configuration changes occur through the PDM server, so the PDMIPC is the only task possible.

Recommended Action

No action is required. Run the **configShow** command to view the configuration file.

Severity

INFO

TRCK-1005

Message

```
<timestamp>, [TRCK-1005], <sequence-number>,, INFO, <system-name>,  
Track-changes on
```

Probable Cause

Indicates that the track change feature has been enabled.

Recommended Action

No action is required. Run the **trackChangesSet 0** command to disable the track change feature.

Severity

INFO

TRCK-1006

Message

```
<timestamp>, [TRCK-1006], <sequence-number>,, INFO, <system-name>,  
Track-changes off
```

Probable Cause

Indicates that the track change feature has been disabled.

Recommended Action

No action is required. Run the **trackChangesSet 1** command to enable the track changes feature.

Severity

INFO

TS Error Messages

TS-1001

Message

```
<timestamp>, [TS-1001], <sequence-number>,, WARNING, <system-name>,  
NTP Query failed: <error code>
```

Probable Cause

Indicates that a network time protocol (NTP) query to the configured external clock server failed. Local clock time on the principal or primary FCS switch is used for fabric synchronization.

This might be logged during temporary operational issues such as IP network connection issues to the external clock server. If it does not recur, it can be ignored.

Recommended Action

Verify that the configured external clock server is available and functional. If that external clock server is not available, choose another.

Severity

WARNING

TS-1002

Message

```
<timestamp>, [TS-1002], <sequence-number>,, WARNING, <system-name>,  
< Type of clock server used > Clock Server used instead of < Type of  
clock server configured >: locl: 0x<code> remote: 0x<code>
```

Probable Cause

Indicates that the fabric time synchronization distributed from the principal or primary FCS switch was not sourced from the *Type of clock server configured*, instead, an alternate server was used, indicated by *Type of clock server used*. The type of clock server used or configured might be either:

- LOCL
Local clock on the principal or primary FCS switch
- External
External NTP server address configured

This might be logged during temporary operational issues such as IP network connection issues to the external clock server or if the fabric is configured for external time synchronization but the principal or primary FCS does not support the feature. If the message does not recur, it should be ignored.

Recommended Action

Run the **tsClockServer** command to verify that the principal or primary FCS switch has the clock server IP configured correctly. Verify that this clock server is accessible to the switch and functional. If the principal or primary FCS does not support the feature, either choose a different switch for the role or reset the clock server to LOCL.

Severity

WARNING

TS-1006

Message

```
<timestamp>, [TS-1006], <sequence-number>,, INFO, <system-name>,  
<message>
```

Probable Cause

Indicates that a time service event is occurring or has failed. The message might be one of the following:

- Init failed. Time Service exiting
Probable Cause: Initialization error, Time Server exits.
- Synchronizing time of day clock
Probable Cause: Usually logged during temporary operational issues when the clock goes out of synchronization: For example, when a time update packet is missed due to fabric reconfiguration or role change of the principal or primary FCS switch. If the message does not recur, it should be ignored.
- Validating time update
Probable Cause: Usually logged during temporary operational issues when a time update packet cannot be validated in a secure fabric. For example, during fabric reconfiguration or role change of the primary FCS switch. If the message does not recur, it should be ignored.

Recommended Action

No action is required.

Severity

INFO

UCST Error Messages

UCST-1003

Message

```
<timestamp>, [UCST-1003], <sequence-number>,, INFO, <system-name>,  
Duplicate Path to Domain <domain ID>, Output Port = <port number>,  
PDB pointer = 0x<value>
```

Probable Cause

Indicates that duplicate paths were reported to the specified domain from the specified output port. The path database (PDB) pointer is the address of the path database and provides debugging information.

Recommended Action

No action is required.

Severity

INFO

UCST-1007

Message

```
<timestamp>, [UCST-1007], <sequence-number>,, CRITICAL,  
<system-name>, Inconsistent route detected: Port = <port number>,  
should be <port number>
```


Probable Cause

Indicates that the switch detected an inconsistency in the routing database between the routing protocol and the hardware configuration. The first port number displayed is what the hardware has configured and the second port number displayed is what the protocol is using.

Recommended Action

Run the **switchDisable** command and then the **switchEnable** command to reset the routing database. Run the **uRouteShow** command to display the new routing tables.

Severity

CRITICAL

UCST-1020

Message

```
<timestamp>, [UCST-1020], <sequence-number>,, WARNING,  
<system-name>, Static route (input-area: <port number>, domain:  
<domain ID> output-area: <port number>) has been ignored due to  
platform limitation.
```

Probable Cause

Indicates that the configured static route cannot be applied to the routing database due to a bloom ASIC hardware limitation.

Recommended Action

No action is required.

Severity

WARNING

UPTH Error Messages

UPTH-1001

Message

```
<timestamp>, [UPTH-1001], <sequence-number>,, WARNING,  
<system-name>, No minimum cost path in candidate list
```

Probable Cause

Indicates that the specified switch is unreachable because no minimum cost path (FSPF UPATH) exists in the candidate list (domain ID list).

Recommended Action

No action is required. This will end the current SPF computation.

Severity

WARNING

USWD Error Messages

USWD-1006

Message

```
<timestamp>, [USWD-1006], <sequence-number>,, WARNING,  
<system-name>, uSWD: <Warning message>
```

Probable Cause

Indicates a warning state in the system. This is an internal use only message.

Recommended Action

No action is required.

Severity

WARNING

WEBD Error Messages

WEBD-1001

Message

```
<timestamp>, [WEBD-1001], <sequence-number>,, WARNING,  
<system-name>, Missing or Invalid Certificate file -- HTTPS is  
configured to be enabled but could not be started.
```

Probable Cause

Indicates that the SSL certificate file is either invalid or absent.

Recommended Action

Run the **configure** command to disable HTTPS. Install a valid key file and enable HTTPS again. For more information on the **configure** command, refer to the *HP StorageWorks Fabric OS 5.x command reference guide*.

Severity

WARNING

WEBD-1002

Message

```
<timestamp>, [WEBD-1002], <sequence-number>,, WARNING,  
<system-name>, Missing or Invalid Key file -- HTTPS is configured to  
be enabled but could not be started.
```

Probable Cause

Indicates that the SSL key file is either invalid or absent.

Recommended Action

Run the **configure** command to disable HTTPS. Install a valid key file and enable HTTPS again. For more information on the **configure** command, refer to the *HP StorageWorks Fabric OS 5.x command reference guide*.

Severity

WARNING

WEBD-1003

Message

```
<timestamp>, [WEBD-1003], <sequence-number>,, INFO, <system-name>,  
HTTP/HTTPS interface disabled
```

Probable Cause

Indicates that the HTTP/HTTPS interface is disabled. This is logged when HTTP/HTTPS is disabled through the **configure** command.

Recommended Action

Run the **configure** command to enable HTTP/HTTPS. For more information on the **configure** command, refer to the *HP StorageWorks Fabric OS 5.x command reference guide*.

Severity

INFO

WEBD-1004

Message

```
<timestamp>, [WEBD-1004], <sequence-number>,, INFO, <system-name>,  
HTTP server will be restarted due to configuration change
```

Probable Cause

Indicates that the HTTP server configuration has changed.

Recommended Action

No action is required.

Severity

INFO

WEBD-1005

Message

```
<timestamp>, [WEBD-1005], <sequence-number>,, WARNING,  
<system-name>, HTTP server will be restarted for logfile truncation
```

Probable Cause

Indicates that the size of HTTP logfile exceeded the maximum limit.

Recommended Action

No action is required.

Severity

WARNING

WEBD-1006

Message

```
<timestamp>, [WEBD-1006], <sequence-number>,, INFO, <system-name>,  
HTTP server restarted due to logfile truncation
```

Probable Cause

Indicates that the size of HTTP logfile exceeded the maximum limit.

Recommended Action

No action is required.

Severity

INFO

WEBD-1007

Message

```
<timestamp>, [WEBD-1007], <sequence-number>,, INFO, <system-name>,  
HTTP server will be restarted due to change of IP Address
```

Probable Cause

Indicates that the IP address of the switch changed and the HTTP server is restarted.

Recommended Action

No action is required.

Severity

INFO

ZOLB Error Messages

ZOLB-1001

Message

```
<timestamp>, [ZOLB-1001], <sequence-number>,, ERROR, <system-name>,  
ZONELIB <error message>
```

Probable Cause

Indicates that there was an internal timeout on the IPC between the name server (NS) and the zoning modules. This usually indicates that the system was busy.

Recommended Action

This message generates core dump files of the related modules (zoned, nsd, rcsd). Copy these core files using the **saveCore** command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

ZONE Error Messages

ZONE-1002

Message

```
<timestamp>, [ZONE-1002], <sequence-number>,, WARNING,  
<system-name>, WWN zoneTypeCheck or zoneGroupCheck warning(<warning  
string>) at port(<port number>)
```

Probable Cause

Indicates that a zone filter or zone group check failure occurred. The frame filter logic reported a failure when creating or adding zone groups during PLOGI trap processing. This messages usually indicates problems when adding CAM entries before the filter setup.

Recommended Action

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

ZONE-1003

Message

```
<timestamp>, [ZONE-1003], <sequence-number>,, WARNING,  
<system-name>, zone(<current zone>) contains (<domain id>, <port  
number>) which does not exist.
```

Probable Cause

Indicates that the port zone member that is targeted for the local switch contains a non-existent port. The effective zoning configuration (displayed in the error message) contains a port number that is out of range.

Recommended Action

Edit the zone database and change the port number to a viable value in the effective configuration.

Severity

WARNING

ZONE-1004

Message

```
<timestamp>, [ZONE-1004], <sequence-number>,, INFO, <system-name>,  
port <port number> enforcement changed to Session Based HARD  
Zoning.
```

Probable Cause

Indicates that the zoning enforcement changed to session-based hard zoning. When a device is zoned using both WWN in one zone and <domain, portarea> in another, this will cause that port to go session based hard zoning.

In session-based zoning, the zone enforcement is checked by the software. In hardware-enforced zoning, zone or alias members are defined using <domain, portarea> exclusively or using WWNs exclusively: that

is, using one method or the other to define all objects in the zoning database. If the devices on the port are defined by a mixture of port IDs and WWNs, the zone enforcement is session based. If the S_ID list of the hardware-enforced zoning overflows (over the S_ID limit), the hardware zone enforcement changes to session-based zoning.

Recommended Action

No action is required.

Severity

INFO

ZONE-1005

Message

```
<timestamp>, [ZONE-1005], <sequence-number>,, INFO, <system-name>,  
HARD & SOFT zones(<zone name>, <zone name>) definitions overlap.
```

Probable Cause

Indicates that a port is zoned with mixed devices (WWN and *<domain, portarea>*). During zoning database cross checking, it is detected that either:

- A port zone member is also listed as a member of a Mixed zone,
- A WWN zone member is also specified as a member of a Mixed zone.

You should use hard zone enforcement whenever possible. Hard zones are more secure than "session-based hard zones". Both types of zones will trap a PLOGI, but hard zones will filter out the I/O frames which “session-based” hard zones do not.

Recommended Action

If hard zone enforcement is preferred, edit the zoning database to have the port zoned with devices defined as either WWN or defined as *<domain, portarea>* but do not mix the methods used to define these zone members.

Severity

INFO

ZONE-1006

Message

```
<timestamp>, [ZONE-1006], <sequence-number>,, WARNING,  
<system-name>, WARNING - WWN(<WWN number>) in HARD PORT zone  
<zone_name>.
```

Probable Cause

Indicates that one or more devices are zoned as WWN devices and also zoned as *<domain, portarea>* devices. The device(s) are used to specify zone members over separate zones.

Recommended Action

If hardware zoning enforcement is preferred, edit the zoning database to have the device zoned using only one specification type, either WWN or *<domain, portarea>*.

Severity

WARNING

ZONE-1007

Message

```
<timestamp>, [ZONE-1007], <sequence-number>,, INFO, <system-name>,  
Ioctl(<function>) in (<error message>) at port (<port number>)  
returns code (<error string>) and reason string (<reason string>)
```

Probable Cause

Indicates that frame filter logic reported a failure during one of the IOCTL calls. The IOCTL call from which the failure is reported is listed as part of the error message. This is usually a programming error when adding CAM entries before the filter setup.

Recommended Action

There are two ways to avoid this problem.

- Avoid having too many hosts zoned with a set of target devices at a single port.
- Avoid having too many zones directed at a single port group on the switch.

Severity

INFO

ZONE-1008

Message

```
<timestamp>, [ZONE-1008], <sequence-number>,, WARNING,  
<system-name>, WARNING - port <port number> Out of CAM entries
```

Probable Cause

Indicates that the total number of entries of S_ID CAM is above the limit while creating or adding a zone group. The maximum number of CAM entries allowed depends on the ASIC.

Recommended Action

If hardware zoning enforcement is preferred, edit the zoning database to have zoned PIDs for that port.

Severity

WARNING

ZONE-1010

Message

```
<timestamp>, [ZONE-1010], <sequence-number>,, WARNING,  
<system-name>, WARNING - Duplicate entries in zone(<zone name>)  
specification.
```

Probable Cause

Indicates that there are duplicate entries in a zone object. A zone object member is specified twice in a given zone object. This message occurs only when enabling a zone configuration.

Recommended Action

Check the members of the zone and delete the duplicate member.

Severity

WARNING

ZONE-1012

Message

```
<timestamp>, [ZONE-1012], <sequence-number>,, WARNING,  
<system-name>, WARNING - All ports are offline.
```

Probable Cause

Indicates that all the ports in a zone are offline.

Recommended Action

Check the device connection.

Severity

WARNING

ZONE-1013

Message

```
<timestamp>, [ZONE-1013], <sequence-number>,, WARNING,  
<system-name>, Quick Loop not supported.
```

Probable Cause

Indicates that the QuickLoop feature is not supported in the current code release. If the QuickLoop zoning configuration is enabled on the switch, it will not be supported.

Recommended Action

Edit the zone database to remove the QuickLoop zoning definition in the effective configuration.

Severity

WARNING

ZONE-1014

Message

```
<timestamp>, [ZONE-1014], <sequence-number>,, ERROR, <system-name>,  
Missing required license - <license name>.
```

Probable Cause

Indicates that the required zoning license is missing.

Recommended Action

Install the zoning license using the **licenseAdd** command. Refer to your switch supplier to obtain a zoning license if you do not have one.

Severity

ERROR

ZONE-1015

Message

```
<timestamp>, [ZONE-1015], <sequence-number>,, WARNING,  
<system-name>, Not owner of the current transaction <transaction  
ID>
```

Probable Cause

Indicates that a zoning change operation is not allowed because the zoning transaction is opened by another task. Indicates concurrent modification of the zone database by multiple administrators.

Recommended Action

Wait until the previous transaction is completed. Verify that only one administrator is working with the zone database at a time.

Severity

WARNING

ZONE-1017

Message

```
<timestamp>, [ZONE-1017], <sequence-number>,, ERROR, <system-name>,  
FA Zone(<zone name>) contains incorrect number of Initiator and  
Target devices
```

Probable Cause

Indicates that the Fabric Assist (FA) zoning configuration has more than one initiator. The probable cause is incorrect entries in the FA zoning configuration.

Recommended Action

Edit the zone database to ensure that only one initiator is set for each FA zone configuration.

Severity

ERROR

ZONE-1018

Message

```
<timestamp>, [ZONE-1018], <sequence-number>,, ERROR, <system-name>,  
Incorrect zoning enforcement type(<zone type>) at port(<port  
number>)
```

Probable Cause

Indicates that an incorrect zoning enforcement type was reported on the specified port. This is a software error. A Quickloop zone type (value = 4) or an uninitialized type (value = 0) are invalid. The valid zone type values are:

- hard port zone (value = 1)
- hard wwn zone (value = 2)
- session based hard zoning (value = 3)
- FA zone (value = 5)

Quickloop zones are not supported in Fabric OS v4.x.

Recommended Action

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

ZONE-1019

Message

```
<timestamp>, [ZONE-1019], <sequence-number>,, ERROR, <system-name>,  
Transaction Commit failed. Reason code <reason code> (<Application  
reason>) - \"<reason string>\"
```

Probable Cause

Indicates that the Reliable Commit Service (RCS) had a transmit error. RCS is a protocol used to transmit changes to the configuration database within a fabric.

Recommended Action

Often this message indicates a transitory problem. Wait a few minutes and retry the command.

Make sure that your changes to the zone database are not overwriting the work of another admin.

Run the **cfgTransShow** command to find out if there is any outstanding transaction running on the local switches.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

ZONE-1022

Message

```
<timestamp>, [ZONE-1022], <sequence-number>,, INFO, <system-name>,  
The effective configuration has changed
```

Probable Cause

Indicates that the effective zone configuration has changed.

Recommended Action

Verify that this zone configuration change was done on purpose. If the new effective zone configuration is correct, no action is necessary.

Severity

INFO

ZONE-1023

Message

```
<timestamp>, [ZONE-1023], <sequence-number>,, INFO, <system-name>,  
Switch connected to port (<port number>) is busy. Retry zone merge
```

Probable Cause

Indicates that the switch is retrying the merge operation. This usually occurs if the switch on the other side of the port is busy.

Recommended Action

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

INFO

ZONE-1024

Message

```
<timestamp>, [ZONE-1024], <sequence-number>,, INFO, <system-name>,  
<Information message>
```

Probable Cause

Indicates that the **cfgSave** command ran successfully. The *<Information message>* is "cfgSave completes successfully."

Recommended Action

No action is required.

Severity

INFO

ZONE-1026

Message

```
<timestamp>, [ZONE-1026], <sequence-number>,, INFO, <system-name>,  
port <port number> Out of CAM entries
```

Probable Cause

Indicates that the total number of S_ID entries while creating or adding a zone group exceeds the limit.

Recommended Action

If hardware zoning enforcement is preferred, edit the zoning database to have zoned PIDs for that port.

Severity

INFO

ZONE-1027

Message

```
<timestamp>, [ZONE-1027], <sequence-number>,, ERROR, <system-name>,  
Zoning transaction aborted - <error reason>
```

Probable Cause

Indicates that the zoning transaction was aborted due to a variety of potential errors. The *error reason* variable can be one of the following:

- Zone Merge Received: The fabric is in the process of merging two zone databases.
- Zone Config update Received: The fabric is in the process of updating the zone database.
- Bad Zone Config: The new config is not viable.
- Zoning Operation failed: A zoning operation failed.
- Shell exited: The command shell has exited.
- Unknown: An error was received for an unknown reason.
- User Command: A user aborted the current zoning transaction.
- Switch Shutting Down: The switch is currently shutting down.

Recommended Action

Many of the causes of this error message are transitory: for example because two admins are working with the zoning database concurrently. If you receive this error, wait a few minutes and try again. Verify that no one else is currently modifying the zone database.

Severity

ERROR

ZONE-1028

Message

```
<timestamp>, [ZONE-1028], <sequence-number>,, WARNING,  
<system-name>, Commit zone DB larger than supported - <zone db size>  
greater than <max zone db size>
```

Probable Cause

Indicates that the zone database size is greater than the limit allowed by the fabric. The limit of the zone database size depends on the lowest level switch in the fabric. Older switches have less memory and force a smaller zone database for the entire fabric.

Recommended Action

Edit the zone database to keep it within the allowable limit for the specific switches in your fabric. Refer to the *HP StorageWorks Fabric OS 5.x administrator guide* for information on the zone database sizes supported for each switch.

Severity

WARNING

ZONE-1029

Message

```
<timestamp>, [ZONE-1029], <sequence-number>,, WARNING,  
<system-name>, Restoring zone cfg from flash failed - bad config  
saved to <config file name> [<return code>]
```

Probable Cause

Indicates that the zone configuration restored from the flash was faulty.

Recommended Action

This error will save the faulty zone configuration in the zoned core file directory. Run the **saveCore** command to save the file.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

WARNING

ZONE-1030

Message

```
<timestamp>, [ZONE-1030], <sequence-number>,, WARNING,  
<system-name>, Converting the zone db for PID format change failed
```

Probable Cause

Indicates that the current zone database could not be converted to reflect the PID format change. Most likely this is caused by the size of the zone database.

Recommended Action

Change the PID format back to its original format. Reduce the size of the zone database. Then you can change the PID format to the requested format.

Severity

WARNING

ZONE-1031

Message

```
<timestamp>, [ZONE-1031], <sequence-number>,, ERROR, <system-name>,  
Switch is in interop mode. (switch, port) members not supported.
```

Probable Cause

The switch is set to interop mode using the **interopMode** command. Interop mode does not allow *<domain, portarea>* members in the active zone database.

Recommended Action

Remove all *<domain, portarea>* members from the zone database, or convert them to WWN zoning.

Severity

ERROR

ZONE-1032

Message

```
<timestamp>, [ZONE-1032], <sequence-number>,, ERROR, <system-name>,  
Domain <domain number> Max Zone DB size <max zone db size>
```

Probable Cause

Indicates that the specified domain does not have enough memory for the the zone database being committed.

Recommended Action

Reduce the size of the zone database and retry the operation.

Severity

ERROR

ZONE-1033

Message

```
<timestamp>, [ZONE-1033], <sequence-number>,, ERROR, <system-name>,  
Domain <domain number> Lowest Max Zone DB size
```

Probable Cause

Indicates that the specified domain has the lowest memory available for the zone database in the fabric. The zone database must be smaller than the memory available on this domain.

Recommended Action

Reduce the size of the zone database and retry the operation.

Severity

ERROR

ZONE-1034

Message

```
<timestamp>, [ZONE-1034], <sequence-number>,, WARNING,  
<system-name>, Corrupted Zoning files detected before reboot,  
currently the file is saved at <config file name>
```

Probable Cause

Indicates that the zone database is corrupt.

Recommended Action

Use the **firmwareDownload** command to reinstall the firmware.

Severity

WARNING

ZONE-1035

Message

```
<timestamp>, [ZONE-1035], <sequence-number>,, ERROR, <system-name>,  
Unable to rename <Old config file name> to <New config file name>:  
error message <System Error Message>
```

Probable Cause

Indicates that the Fabric OS cannot rename the zone configuration file. Typically the zone configuration is too large for the memory available on the switch.

Recommended Action

Reduce the size of the zone database and retry the operation.

Severity

ERROR

ZONE-1036

Message

```
<timestamp>, [ZONE-1036], <sequence-number>,, ERROR, <system-name>,  
Unable to create <config file name>: error message <System Error  
Message>
```

Probable Cause

Indicates that the Fabric OS cannot create the zone configuration file. Typically the zone configuration is too large for the memory available on the switch.

Recommended Action

Reduce the size of the zone database and retry the operation.

Severity

ERROR

ZONE-1037

Message

```
<timestamp>, [ZONE-1037], <sequence-number>,, ERROR, <system-name>,  
Unable to examine <config file name>: error message <System Error  
Message>
```

Probable Cause

Indicates that the Fabric OS cannot examine the zone configuration file. Typically the zone configuration is too large for the memory available on the switch.

Recommended Action

Reduce the size of the zone database and retry the operation.

Severity

ERROR

ZONE-1038

Message

```
<timestamp>, [ZONE-1038], <sequence-number>,, ERROR, <system-name>,  
Unable to allocate memory for <config file name>: error message  
<System Error Message>
```

Probable Cause

Indicates that the Fabric OS cannot allocate enough memory for the zone configuration file. Typically the zone configuration is too large for the memory available on the switch.

Recommended Action

Reduce the size of the zone database and retry the operation.

Severity

ERROR

ZONE-1039

Message

```
<timestamp>, [ZONE-1039], <sequence-number>,, ERROR, <system-name>,  
Unable to read contents of <config file name>: error message <System  
Error Message>
```

Probable Cause

Indicates that the Fabric OS cannot read the zone configuration file. Typically the zone configuration is too large for the memory available on the switch.

Recommended Action

Reduce the size of the zone database and retry the operation.

Severity

ERROR

ZONE-1040

Message

```
<timestamp>, [ZONE-1040], <sequence-number>,, INFO, <system-name>,  
Merged zone database exceeds limit.
```

Probable Cause

Indicates that the Fabric OS cannot read the merged zone configuration file. Typically the zone configuration is too large for the memory available on the switch.

Recommended Action

Reduce the size of the zone database and retry the operation.

Severity

INFO

ZONE-1041

Message

```
<timestamp>, [ZONE-1041], <sequence-number>,, WARNING,  
<system-name>,Unstable link detected during merge at port <Port  
number>.
```

Probable Cause

Indicates a possible unstable link, or faulty cable.

Recommended Action

Check the SFP and cable at the specified port and verify that they are not faulty. Replace the SFP and cable as necessary.

Severity

WARNING

ZONE-3001

Message

```
<timestamp>, [ZONE-3001], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: <Zone object type> \"<Zone  
object member list>\" added to <Zone object set type> \"<Zone object  
set name>\".
```

Probable Cause

Indicates that a new zone object member or members have been added to a zone object set.

A zone object may be an alias, zone member, zone or zone configuration. The string "..." appears at the end of the zone object member list if the list was truncated in the message.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

ZONE-3002

Message

```
<timestamp>, [ZONE-3002], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: <Zone object set type> \"<Zone  
object set name>\" created with <Zone object type> \"<Zone object  
member list>\".
```

Probable Cause

Indicates that a new zone object set was created with the specified zone object member or members added.

A zone object may be an alias, zone member, zone or zone configuration. The string "..." appears at the end of the zone object member list if the list was truncated in the message.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

ZONE-3003

Message

```
<timestamp>, [ZONE-3003], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: <Zone object type> \"<Zone  
object name>\" deleted.
```

Probable Cause

Indicates that a zone object has been deleted.

A zone object may be an alias, zone member, zone, or zone configuration.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

ZONE-3004

Message

```
<timestamp>, [ZONE-3004], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: <Zone object type> \"<Zone  
object member list>\" removed from <Zone object set type> \"<Zone  
object set name>\".
```

Probable Cause

Indicates that zone object member or members have been removed from a zone object set.

A zone object may be an alias, zone member, zone or zone configuration. The string "..." appears at the end of the zone object member list if the list was truncated in the message.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

ZONE-3005

Message

```
<timestamp>, [ZONE-3005], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: All zone information cleared  
from transaction buffer.
```

Probable Cause

Indicates that all zone information has been cleared from the transaction buffer.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

ZONE-3006

Message

```
<timestamp>, [ZONE-3006], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: Current zone configuration  
disabled.
```

Probable Cause

Indicates that the current zone configuration has been disabled.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

ZONE-3007

Message

```
<timestamp>, [ZONE-3007], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: Zone configuration \"<Zone  
configuration>\" enabled.
```

Probable Cause

Indicates that a zone configuration has been enabled.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

ZONE-3008

Message

```
<timestamp>, [ZONE-3008], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: Current zone configuration  
saved to flash.
```

Probable Cause

Indicates that the current zone configuration has been saved to flash.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

ZONE-3009

Message

```
<timestamp>, [ZONE-3009], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: <Event Description>
```

Probable Cause

Indicates that a zone transaction has been aborted.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

ZONE-3010

Message

```
<timestamp>, [ZONE-3010], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: Zone object \"<Zone object  
name>\" copied to new zone object \"<New Zone object name>\".
```

Probable Cause

Indicates that a zone object has been copied to a new zone object.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

ZONE-3011

Message

```
<timestamp>, [ZONE-3011], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: Zone object \"<Zone object  
name>\" expunged.
```

Probable Cause

Indicates that a zone object has been expunged.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

ZONE-3012

Message

```
<timestamp>, [ZONE-3012], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: Zone object \"<Zone object  
name>\" renamed to \"<New Zone object name>\".
```

Probable Cause

Indicates that a zone object has been renamed.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

Index

A

- audience 77
- audit logging 82
- AUTH-1001 95
- AUTH-1003 95
- AUTH-1004 96
- AUTH-1005 96
- AUTH-1006 96
- AUTH-1007 97
- AUTH-1008 97
- AUTH-1010 97
- AUTH-1011 98
- AUTH-1012 98
- AUTH-1013 99
- AUTH-1014 99
- AUTH-1017 99
- AUTH-1018 100
- AUTH-1020 100
- AUTH-1022 101
- AUTH-1023 101
- AUTH-1025 102
- AUTH-1027 102
- AUTH-1028 103
- AUTH-1029 103
- AUTH-1030 103
- AUTH-1031 104
- AUTH-1032 104
- AUTH-1033 105
- AUTH-1034 105
- AUTH-1035 105
- AUTH-1036 106
- AUTH-1037 106
- AUTH-1038 107
- authorized reseller, HP 79

B

- BL-1001 107
- BL-1002 108
- BL-1003 108
- BL-1004 109
- BL-1006 109
- BL-1007 109
- BL-1008 110
- BL-1009 110
- BL-1010 111
- BL-1011 111
- BL-1012 112
- BL-1013 112
- BL-1014 113
- BL-1015 113
- BL-1016 114

C

- clearing the system message log 88
- conventions
 - document 78
 - text symbols 78

D

- document
 - conventions 78
 - related documentation 77
- dual-CP systems 83
- dumping the system messages 87

E

- EM-1002 118
- EM-1003 118
- EM-1004 119
- EM-1005 119
- EM-1006 120
- EM-1007 120
- EM-1008 121
- EM-1009 121
- EM-1010 122
- EM-1011 122
- EM-1012 122
- EM-1013 123
- EM-1014 124
- EM-1015 124
- EM-1016 125
- EM-1017 125, 126
- EM-1028 126
- EM-1029 127
- EM-1031 128
- EM-1033 128
- EM-1034 128, 129
- EM-1036 130
- EM-1041 130
- EM-1042 131
- EM-1043 132
- EM-1044 132
- EM-1045 132
- EM-1046 133
- EM-1047 133
- EM-1048 134
- EM-1049 134
- EM-1050 135
- EM-1051 136
- EM-1052 136
- EM-1053 137
- EM-1055 138
- EM-1056 138, 139
- example system message 85

F

FABR-1002	140	FSS-1003	169
FABR-1003	141	FSS-1004	169
FABR-1004	141	FSS-1005	170
FABR-1005	142	FSS-1006	170
FABR-1006	142	FSSM-1003	171
FABR-1007	142	FSSM-1004	171
FABR-1008	143	FW-1001	171
FABR-1009	143	FW-1002	172
FABR-1010	144	FW-1003	172
FABR-1011	144	FW-1004	173
FABR-1012	144	FW-1005	173
FABR-1013	145	FW-1006	173
FABR-1014	145	FW-1007	174
FABR-1015	145	FW-1008	174
FABR-1016	146	FW-1009	174
FABR-1017	146	FW-1010	175
FABR-1018	146	FW-1011	175
FABR-1019	147	FW-1012	175
FABR-1020	147	FW-1033	176
FABR-1021	148	FW-1034	176
FABR-1022	148	FW-1035	176
FABR-1023	149	FW-1036	177
FABR-1024	149	FW-1037	177
FABR-1029	149	FW-1038	177
FABR-1030	150	FW-1039	178
FABS-1002	150	FW-1040	178
FABS-1004	151	FW-1041	179
FABS-1005	151	FW-1042	179
FABS-1006	152	FW-1043	179
FABS-1007	152	FW-1044	180
FABS-1008	153	FW-1045	180
FABS-1009	153	FW-1046	180
FABS-1010	153	FW-1047	181
FABS-1011	154	FW-1048	181
FABS-1012	154	FW-1049	181
FABS-1013	154	FW-1050	182
FABS-1014	155	FW-1051	182
FABS-1015	155	FW-1052	182
FCPD-1001	156	FW-1113	183
FCPD-1002	156	FW-1114	183
FCPD-1003	157	FW-1115	184
FICU-1002	158, 161	FW-1116	184
FICU-1003	158, 162	FW-1117	184
FICU-1004	159, 162	FW-1118	185
FICU-1005	159, 163	FW-1119	185
FICU-1006	160, 163	FW-1120	186
FICU-1007	160, 163	FW-1121	186
FICU-1008	160, 164	FW-1122	187
FICU-1009	161, 164	FW-1123	187
FLOD-1003	165	FW-1124	187
FLOD-1004	165	FW-1125	188
FLOD-1005	166	FW-1126	188
FLOD-1006	166	FW-1127	189
FSPF-1002	167	FW-1128	189
FSPF-1003	167	FW-1129	190
FSPF-1005	167	FW-1130	190
FSPF-1006	168	FW-1131	190
FSS-1002	168	FW-1132	191
		FW-1133	191

FW-1134	191	FW-1272	214
FW-1135	192	FW-1273	214
FW-1136	192	FW-1274	214
FW-1137	192	FW-1275	215
FW-1138	193	FW-1296	215
FW-1139	193	FW-1297	216
FW-1140	194	FW-1298	216
FW-1160	194	FW-1299	216
FW-1161	194	FW-1300	217
FW-1162	195	FW-1301	217
FW-1163	195	FW-1302	218
FW-1164	196	FW-1303	218
FW-1165	196	FW-1304	218
FW-1166	196	FW-1305	219
FW-1167	197	FW-1306	219
FW-1168	197	FW-1307	220
FW-1169	197	FW-1308	220
FW-1170	198	FW-1309	220
FW-1171	198	FW-1310	221
FW-1172	199	FW-1311	221
FW-1173	199	FW-1312	221
FW-1174	199	FW-1313	222
FW-1175	200	FW-1314	222
FW-1176	200	FW-1315	223
FW-1177	200	FW-1316	223
FW-1178	201	FW-1317	223
FW-1179	201	FW-1318	224
FW-1180	201	FW-1319	224
FW-1181	202	FW-1320	225
FW-1182	202	FW-1321	225
FW-1183	202	FW-1322	225
FW-1184	203	FW-1323	226
FW-1185	203	FW-1324	226
FW-1186	204	FW-1325	227
FW-1187	204	FW-1326	227
FW-1188	204	FW-1327	227
FW-1189	205	FW-1328	228
FW-1190	205	FW-1329	228
FW-1191	205	FW-1330	228
FW-1192	206	FW-1331	229
FW-1193	206	FW-1332	229
FW-1194	207	FW-1333	230
FW-1195	207	FW-1334	230
FW-1216	207	FW-1335	230
FW-1217	208	FW-1336	231
FW-1218	208	FW-1337	231
FW-1219	209	FW-1338	232
FW-1240	209	FW-1339	232
FW-1241	209	FW-1340	232
FW-1242	210	FW-1341	233
FW-1243	210	FW-1342	233
FW-1244	211	FW-1343	234
FW-1245	211	FW-1344	234
FW-1246	211	FW-1345	234
FW-1247	212	FW-1346	235
FW-1248	212	FW-1347	235
FW-1249	212	FW-1348	236
FW-1250	213	FW-1349	236
FW-1251	213	FW-1350	236

FW-1351 [237](#)
FW-1352 [237](#)
FW-1353 [238](#)
FW-1354 [238](#)
FW-1355 [239](#)
FW-1356 [239](#)
FW-1357 [239](#)
FW-1358 [240](#)
FW-1359 [240](#)
FW-1360 [241](#)
FW-1361 [241](#)
FW-1362 [241](#)
FW-1363 [242](#)
FW-1364 [242](#)
FW-1365 [242](#)
FW-1366 [243](#)
FW-1367 [243](#)
FW-1368 [243](#)
FW-1369 [244](#)
FW-1370 [244](#)
FW-1371 [245](#)
FW-1372 [245](#)
FW-1373 [245](#)
FW-1374 [246](#)
FW-1375 [246](#)
FW-1376 [247](#)
FW-1377 [247](#)
FW-1378 [247](#)
FW-1379 [248](#)
FW-1400 [248](#)
FW-1401 [249](#)
FW-1402 [249](#)
FW-1403 [249](#)
FW-1424 [250](#)
FW-1425 [250](#)
FW-1426 [250](#)
FW-1427 [251](#)
FW-1428 [251](#)
FW-1429 [251](#)
FW-1430 [252](#)
FW-1431 [252](#)
FW-1432 [252](#)
FW-1433 [253](#)
FW-1434 [253](#)
FW-1435 [254](#)
FW-1436 [254](#)
FW-1437 [254](#)
FW-1438 [255](#)
FW-1439 [255](#)
FW-1440 [255](#)
FW-1441 [256](#)
FW-1442 [256](#)
FW-1443 [256](#)
FW-1444 [257](#)

G

gathering information about the problem [89](#)

H

HAM-1002 [257](#)
HAM-1004 [258](#)
HAMK-1003 [259](#)
help, obtaining [79](#)
HIL-1101 [260](#)
HIL-1102 [260](#)
HIL-1103 [260](#)
HIL-1104 [261](#)
HIL-1105 [261](#)
HIL-1106 [261](#)
HIL-1107 [262](#)
HIL-1108 [262](#)
HIL-1201 [263](#)
HIL-1202 [263](#)
HIL-1203 [264](#)
HIL-1204 [264](#)
HIL-1205 [265](#)
HIL-1206 [265](#)
HIL-1207 [266](#)
HIL-1301 [266](#)
HIL-1302 [267](#)
HIL-1303 [267](#)
HIL-1304 [268](#)
HIL-1305 [268](#)
HIL-1306 [268](#)
HIL-1307 [269](#)
HIL-1308 [269](#)
HIL-1309 [270](#)
HIL-1310 [270](#)
HIL-1401 [271](#)
HIL-1402 [271](#)
HIL-1403 [271](#)
HIL-1404 [272](#)
HIL-1501 [272](#)
HIL-1502 [272](#)
HIL-1503 [273](#)
HIL-1504 [273](#)
HIL-1505 [274](#)
HIL-1506 [274](#)
HIL-1507 [275](#)
HIL-1508 [275](#)
HIL-1509 [276](#)
HIL-1601 [276](#)
HIL-1602 [276](#)
HLO-1002 [277](#)
HLO-1003 [278](#)
HMON-1001 [278](#)
HP
authorized reseller [79](#)
storage web site [79](#)
Subscriber's choice web site [79](#)
technical support [79](#)

K

KTRC-1001 [279](#)
KTRC-1002 [280](#)
KTRC-1003 [280](#)

KTRC-1004 [280](#)

L

LOG-1000 [281](#)

LOG-1001 [281](#)

LOG-1002 [281](#)

looking up a system message [88](#)

LSDB-1001 [282](#)

LSDB-1002 [282](#)

LSDB-1003 [282](#)

LSDB-1004 [283](#)

M

message severity levels [81](#)

MFIC-1001 [283](#)

MFIC-1002 [284](#)

MFIC-1003 [284](#)

MPTH-1001 [284](#)

MPTH-1002 [285](#)

MPTH-1003 [285](#)

MQ-1004 [285](#)

MS-1001 [286](#)

MS-1002 [286](#)

MS-1003 [287](#)

MS-1004 [288](#)

MS-1005 [288](#)

MS-1006 [289](#)

MS-1008 [289](#)

MS-1021 [289](#)

N

NBFS-1001 [290](#)

NBFS-1002 [290](#)

NBFS-1003 [291](#)

NS-1001 [291](#)

NS-1002 [292](#)

NS-1003 [292](#)

NS-1004 [292](#)

O

overview of the system messages [81](#)

P

panic dump and core dump files [83](#)

PDM-1001 [293](#)

PDM-1002 [293](#)

PDM-1003 [294](#)

PDM-1004 [294](#)

PDM-1005 [294](#)

PDM-1006 [295](#)

PDM-1007 [295](#)

PDM-1008 [295](#)

PDM-1009 [296](#)

PDM-1010 [296](#)

PDM-1011 [296](#)

PDM-1012 [297](#)

PDM-1013 [297](#)

PDM-1014 [297](#)

PDM-1017 [298](#)

PDM-1019 [298](#)

PDM-1020 [299](#)

PDM-1021 [299](#)

PDTR-1001 [299](#)

PDTR-1002 [300](#)

PLAT-1000 [300](#)

Port Logs [83](#)

PORT-1003 [301](#)

PORT-1004 [301](#)

PS-1000 [302](#)

PS-1001 [302](#)

PS-1002 [302](#)

PS-1003 [303](#)

PS-1004 [303](#)

PS-1005 [303](#)

PSWP-1001 [304](#)

PSWP-1002 [304](#)

PSWP-1003 [304](#)

PSWP-1004 [305](#)

R

rack stability, warning [79](#)

RCS-1001 [305](#)

RCS-1002 [305](#)

RCS-1003 [306](#)

RCS-1004 [306](#)

RCS-1005 [307](#)

RCS-1006 [307](#)

RCS-1007 [307](#)

RCS-1008 [308](#)

reading a system message [85](#)

related documentation [77](#)

responding to a system message [88](#)

RPCD-1001 [308](#)

RPCD-1002 [308](#)

RPCD-1003 [309](#)

RPCD-1004 [309](#)

RPCD-1005 [309](#)

RPCD-1006 [310](#)

RPCD-1007 [310](#)

RTWR-1001 [310](#), [311](#)

RTWR-1002 [311](#)

S

SCN-1001 [312](#)

SEC-1001 [312](#)

SEC-1002 [313](#)

SEC-1003 [313](#)

SEC-1005 [314](#)

SEC-1006 [314](#)

SEC-1007 [314](#)

SEC-1008 [315](#)

SEC-1009 [315](#)

SEC-1016 [315](#)

SEC-1022 [316](#)

SEC-1024 [316](#)

SEC-1025 [316](#)

SEC-1026 [317](#)

SEC-1028 [317](#)
SEC-1029 [318](#)
SEC-1030 [318](#)
SEC-1031 [318](#)
SEC-1032 [319](#)
SEC-1033 [319](#)
SEC-1034 [319](#)
SEC-1035 [320](#)
SEC-1036 [320](#)
SEC-1037 [320](#)
SEC-1038 [321](#)
SEC-1040 [321](#)
SEC-1041 [321](#)
SEC-1042 [322](#)
SEC-1043 [322](#)
SEC-1044 [322](#)
SEC-1045 [323](#)
SEC-1046 [323](#)
SEC-1049 [324](#)
SEC-1050 [324](#)
SEC-1051 [324](#)
SEC-1052 [325](#)
SEC-1053 [325](#)
SEC-1054 [325](#)
SEC-1055 [326](#)
SEC-1056 [326](#)
SEC-1057 [327](#)
SEC-1059 [327](#)
SEC-1062 [327](#)
SEC-1063 [328](#)
SEC-1064 [328](#)
SEC-1065 [328](#)
SEC-1069 [329](#)
SEC-1071 [329](#)
SEC-1072 [329](#)
SEC-1073 [330](#)
SEC-1074 [330](#)
SEC-1075 [330](#)
SEC-1076 [331](#)
SEC-1077 [331](#)
SEC-1078 [331](#)
SEC-1079 [332](#)
SEC-1080 [332](#)
SEC-1081 [332](#)
SEC-1082 [333](#)
SEC-1083 [333](#)
SEC-1084 [333](#)
SEC-1085 [334](#)
SEC-1086 [334](#)
SEC-1088 [334](#)
SEC-1089 [335](#)
SEC-1090 [335](#)
SEC-1091 [336](#)
SEC-1092 [336](#)
SEC-1093 [336](#)
SEC-1094 [337](#)
SEC-1095 [337](#)
SEC-1096 [337](#)
SEC-1097 [338](#)

SEC-1098 [338](#)
SEC-1099 [338](#)
SEC-1100 [339](#)
SEC-1101 [339](#)
SEC-1102 [339](#)
SEC-1104 [340](#)
SEC-1105 [340](#)
SEC-1106 [341](#)
SEC-1107 [341](#)
SEC-1108 [341](#)
SEC-1110 [342](#)
SEC-1111 [342](#)
SEC-1112 [342](#)
SEC-1115 [343](#)
SEC-1116 [343](#)
SEC-1117 [343](#)
SEC-1118 [344](#)
SEC-1119 [344](#)
SEC-1121 [344](#)
SEC-1122 [345](#)
SEC-1123 [345](#)
SEC-1124 [345](#)
SEC-1126 [346](#)
SEC-1130 [346](#)
SEC-1135 [346](#)
SEC-1136 [347](#)
SEC-1137 [347](#)
SEC-1138 [347](#)
SEC-1139 [348](#)
SEC-1142 [348](#)
SEC-1145 [349](#)
SEC-1146 [349](#)
SEC-1153 [349](#)
SEC-1154 [350](#)
SEC-1155 [350](#)
SEC-1156 [351](#)
SEC-1157 [351](#)
SEC-1158 [351](#)
SEC-1159 [352](#)
SEC-1160 [352](#)
SEC-1163 [352](#)
SEC-1164 [353](#)
SEC-1165 [353](#)
SEC-1166 [353](#)
SEC-1167 [354](#)
SEC-1168 [354](#)
SEC-1170 [354](#)
SEC-1171 [355](#)
SEC-1172 [355](#)
SEC-1173 [355](#)
SEC-1174 [356](#)
SEC-1175 [356](#)
SEC-1176 [356](#)
SEC-1180 [357](#)
SEC-1181 [357](#)
SEC-1182 [357](#)
SEC-1183 [358](#)
SEC-1184 [358](#)
SEC-1185 [358](#)

SEC-1186 [359](#)
 SEC-1187 [359](#)
 SEC-1188 [359](#)
 SEC-1189 [360](#)
 SEC-1190 [360](#)
 SEC-1191 [361](#)
 SEC-1192 [361](#)
 SEC-1193 [361](#)
 SEC-1194 [362](#)
 SEC-1195 [362](#)
 SEC-1196 [362](#)
 SEC-1197 [363](#)
 SEC-1198 [363](#)
 SEC-1199 [363](#)
 SEC-1200 [364](#)
 SEC-1201 [364](#)
 SEC-1202 [365](#)
 SEC-1250 [365](#)
 SEC-1251 [365](#)
 SEC-1253 [366](#)
 SEC-1300 [366](#)
 SEC-1301 [366](#)
 SEC-1302 [367](#)
 SEC-1303 [367](#)
 SEC-1304 [367](#)
 SEC-1305 [368](#)
 SEC-1306 [368](#)
 SEC-1307 [368](#)
 SEC-1308 [369](#)
 SEC-3001 [369](#)
 SEC-3002 [370](#)
 SEC-3003 [370](#)
 SEC-3004 [371](#)
 SEC-3005 [371](#)
 SEC-3006 [371](#)
 SEC-3007 [372](#)
 SEC-3008 [372](#)
 SEC-3009 [372](#)
 SEC-3010 [373](#)
 SEC-3011 [373](#)
 SEC-3012 [374](#)
 SEC-3013 [374](#)
 SEC-3014 [374](#)
 SEC-3015 [375](#)
 SEC-3016 [375](#)
 SEC-3017 [375](#)
 SNMP-1001 [376](#)
 SNMP-1002 [376](#)
 SNMP-1003 [376](#)
 SNMP-1004 [377](#)
 SS-1000 [377](#)
 SS-1001 [377](#)
 Subscriber's choice, HP [79](#)
 SULB-1001 [378](#)
 SULB-1002 [378](#)
 SULB-1003 [378](#)
 SULB-1005 [379](#)
 SULB-1006 [379](#)
 SULB-1007 [379](#)

SULB-1008 [380](#)
 SULB-1009 [380](#)
 SULB-1010 [384](#)
 supportSave command [84](#)
 SWCH-1001 [385](#)
 SWCH-1002 [385](#)
 SWCH-1003 [385](#)
 SWCH-1004 [386](#)
 SWCH-1005 [386](#)
 symbols in text [78](#)
 SYSC-1001 [387](#)
 SYSC-1002 [387](#)
 SYSM-1001 [388](#)
 SYSM-1002 [388](#)
 SYSM-1003 [389](#)
 SYSM-1004 [389](#)
 system console [84](#)
 system logging daemon [83](#)
 system message log (RASlog) [82](#)
 system module descriptions [89](#)

T

technical support, HP [79](#)
 text symbols [78](#)
 trace dumps [84](#)
 TRCE-1001 [389](#)
 TRCE-1002 [390](#)
 TRCE-1003 [390](#)
 TRCE-1004 [391](#)
 TRCE-1005 [391](#)
 TRCE-1006 [391](#)
 TRCE-1007 [392](#)
 TRCE-1008 [392](#)
 TRCE-1009 [393](#)
 TRCE-1010 [393](#)
 TRCE-1011 [393](#)
 TRCK-1001 [394](#)
 TRCK-1002 [394](#)
 TRCK-1003 [394](#)
 TRCK-1004 [395](#)
 TRCK-1005 [395](#)
 TRCK-1006 [395](#)
 TS-1001 [396](#)
 TS-1002 [396](#)
 TS-1006 [397](#)

U

UCST-1003 [397](#)
 UCST-1007 [398](#)
 UCST-1020 [398](#)
 UPTH-1001 [398](#)
 USWD-1006 [399](#)

V

view or configure the system message logs [84](#)
 viewing system messages from Web Tools [87](#)
 viewing the system messages with page breaks [88](#)

W

warning

rack stability [79](#)

web sites

HP storage [79](#)

HP Subscriber's choice [79](#)

WEBD-1001 [399](#)

WEBD-1002 [399](#)

WEBD-1003 [400](#)

WEBD-1004 [400](#)

WEBD-1005 [400](#)

WEBD-1006 [401](#)

WEBD-1007 [401](#)

Z

ZOLB-1001 [401](#)

ZONE-1002 [402](#)

ZONE-1003 [402](#)

ZONE-1004 [402](#)

ZONE-1005 [403](#)

ZONE-1006 [403](#)

ZONE-1007 [404](#)

ZONE-1008 [404](#)

ZONE-1010 [404](#)

ZONE-1012 [405](#)

ZONE-1013 [405](#)

ZONE-1014 [405](#)

ZONE-1015 [406](#)

ZONE-1017 [406](#)

ZONE-1018 [406](#)

ZONE-1019 [407](#)

ZONE-1022 [407](#)

ZONE-1023 [408](#)

ZONE-1024 [408](#)

ZONE-1026 [408](#)

ZONE-1027 [409](#)

ZONE-1028 [409](#)

ZONE-1029 [410](#)

ZONE-1030 [410](#)

ZONE-1031 [410](#)

ZONE-1032 [411](#)

ZONE-1033 [411](#)

ZONE-1034 [411](#)

ZONE-1035 [412](#)

ZONE-1036 [412](#)

ZONE-1037 [412](#)

ZONE-1038 [413](#)

ZONE-1039 [413](#), [414](#)

ZONE-3001 [414](#)

ZONE-3002 [414](#)

ZONE-3003 [415](#)

ZONE-3004 [415](#)

ZONE-3005 [416](#)

ZONE-3006 [416](#)

ZONE-3007 [416](#)

ZONE-3008 [417](#)

ZONE-3009 [417](#)

ZONE-3010 [417](#)

ZONE-3011 [418](#)

ZONE-3012 [418](#)